THE AMERICAN MATHEMATICAL MONTHLY

Volume 106, Number 4 April 1999

AN OFFICIAL PUBLICATION OF THE MATHEMATICAL ASSOCIATION OF AMERICA

NOTICE TO AUTHORS

The MONTHLY publishes articles, as well as notes and other features, about mathematics and the profession. Its readers span a broad spectrum of mathematical interests, and include professional mathematicians as well as students of mathematics at all collegiate levels. Authors are invited to submit articles and notes that bring interesting mathematical ideas to a wide audience of MONTHLY readers.

The MONTHLY's readers expect a high standard of exposition; they expect articles to inform, stimulate, challenge, enlighten, and even entertain. MONTHLY articles are meant to be read, enjoyed, and discussed, rather than just archived. Articles may be expositions of old or new results, historical or biographical essays, speculations or definitive treatments, broad developments, or explorations of a single application. Novelty and generality are far less important than clarity of exposition and broad appeal. Appropriate figures, diagrams, and photographs are encouraged.

Notes are short, sharply focussed, and possibly informal. They are often gems that provide a new proof of an old theorem, a novel presentation of a familiar theme, or a lively discussion of a single issue.

Articles and Notes should be sent to the Editor:

ROGER A. HORN
1515 Mineral Square, Room 142
University of Utah
Salt Lake City, UT 84112

Please send your email address and 3 copies of the complete manuscript (including all figures with captions and lettering), typewritten on only one side of the paper. In addition, send one original copy of all figures without lettering, drawn carefully in black ink on separate sheets of paper. Authors who use LaTeX are urged to use article.sty and its standard environments with no custom formatting.

Letters to the Editor on any topic are invited; please send to the MONTHLY's Utah office. Comments, criticisms, and suggestions for making the MONTHLY more lively, entertaining, and informative are welcome.

See the MONTHLY section of MAA Online for current information such as contents of issues and descriptive summaries of forthcoming articles:

http://www.maa.org/

Proposed problems or solutions should be sent to:

DANIEL ULLMAN, MONTHLY Problems
Department of Mathematics
The George Washington University
2201 G Street, NW, Room 428A
Washington, DC 20052

Please send 2 copies of all problems/solutions material, typewritten on only one side of the paper.

Reprint permission:
DONALD ALBERS, Director of Publication

Advertising Correspondence:
Dave Riska, *driska@maa.org*

Change of address, missing issues inquiries, and other subscription correspondence:
MAA Service Center, *maahq@maa.org*

All at the address:

The Mathematical Association of America
1529 Eighteenth Street, N.W.
Washington, DC 20036

Recent copies of the Monthly are available for purchase through the MAA's customer service center. email: maahq@maa.org; phone: 1-800-331-1622

Microfilm Editions: University Microfilms International, Serial Bid coordinator, 300 North Zeeb Road, Ann Arbor, MI 48106.

The AMERICAN MATHEMATICAL MONTHLY (ISSN 0002-9890) is published monthly except bimonthly June-July and August-September by the Mathematical Association of America at 1529 Eighteenth Street, N.W., Washington, DC 20036 and Montpelier, VT. Second class postage paid at Washington, DC, and additional mailing offices. ***Postmaster***: Send address changes to the American Mathematical Monthly, Membership / Subscription Department, MAA, 1529 Eighteenth Street, N.W., Washington, DC, 20036-1385.

The Mandelbrot Set, the Farey Tree, and the Fibonacci Sequence

Robert L. Devaney

1. INTRODUCTION. Our goal is to explain and to make precise several "folk theorems" involving the Mandelbrot set and the Farey tree [**4**].

The *Mandelbrot set* is a subset of the parameter plane for iteration of the complex quadratic function $Q_c(z) = z^2 + c$. Here the parameter c is complex. The Mandelbrot set $\mathcal{M}$ consists of those c values for which the *orbit* of 0—the sequence $0, Q_c(0), Q_c(Q_c(0)) = Q_c^2(0), Q_c^3(0), \ldots$ —is bounded.

One reason for singling out the orbit of 0 is the following important fact from complex dynamics: If Q_c possesses an attracting cycle, then the orbit of 0, the critical point, must converge to that cycle [**3**]; a *cycle* is an orbit $z_0, Q_c(z_0), \ldots, Q_c^n(z_0) = z_0$ that returns to itself after n iterations. A cycle is called *attracting* if all sufficiently nearby points have orbits that tend to the cycle.

Since the orbit of 0 tends to any attracting cycle of Q_c, it follows that Q_c admits at most one attracting cycle. Also, a c-value for which Q_c has an attracting cycle must lie in $\mathcal{M}$ since the orbit of 0 is bounded. In fact, the c-values for which Q_c has an attracting cycle comprise all of the visible interior of the Mandelbrot set. By visible, we mean that nobody has ever found experimentally or otherwise a component of the interior that does not have this property. One of the main conjectures concerning $\mathcal{M}$ is that its interior consists *only* of c-values for which there is an attracting cycle.

The Mandelbrot set features a basic cardioid shape from which hang numerous "bulbs" or "decorations"; see Figure 1. Each of these bulbs is a large disk that is directly attached to the cardioid, together with numerous other smaller decorations and a prominent "antenna."

Each of these large disks turns out to contain c-values for which Q_c admits an attracting cycle with period q and rotation number p/q. That is, the attracting cycle of Q_c tends to rotate about a central fixed point, turning on average p/q revolutions at each iteration. For this reason, this bulb is called the p/q bulb. Each of the c-values in this bulb has essentially the same dynamical behavior.

A perhaps surprising folk theorem says that we can recognize the p/q-bulb from the geometry of the bulb itself. That is, we can read off dynamical information from the geometric information contained in the Mandelbrot set.

For example, the $2/5$ bulb is displayed in Figure 2. For any c-value in this large disk, Q_c features an attracting cycle with rotation number $2/5$. The $2/5$ bulb possesses an antenna-like structure that features a junction point from which five spokes emanate. One of these spokes is attached directly to the $2/5$ bulb; we call this spoke the *principal spoke*. Now look at the "smallest" of the non-principal spokes. Note that this spoke is located, roughly speaking, $2/5$ of a turn in the counterclockwise direction from the principal spoke. This is how we identify this bulb as the $2/5$-bulb.

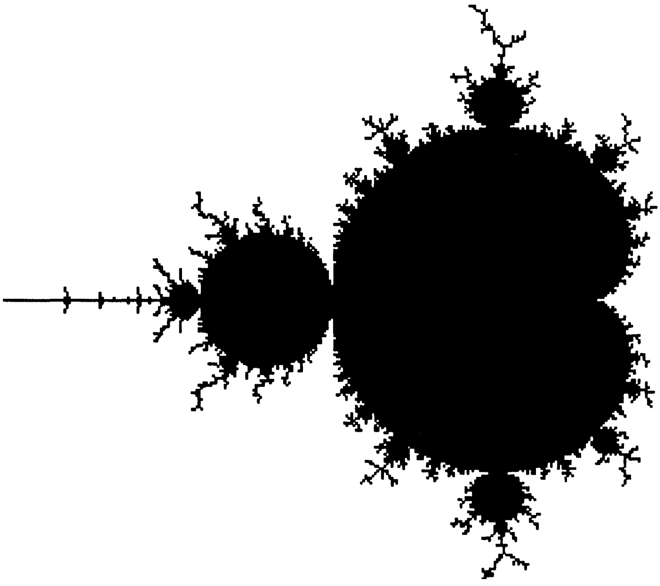


Figure 1. The Mandelbrot set.

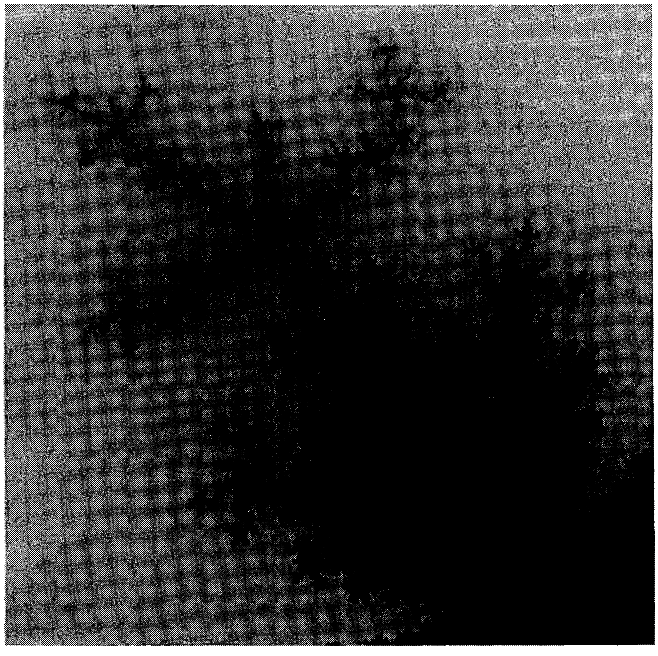


Figure 2. The $2/5$ bulb.

As another example, in Figure 3 we display the $3/7$ bulb. This bulb has 7 spokes emanating from the junction point, and the smallest is located $3/7$ of a turn in the counterclockwise direction from the principal spoke. This then is the folk theorem: You can recognize the p/q bulb by locating the "smallest" spoke in the antenna and determining its location relative to the principal spoke. Of course, the word "smallest" needs some clarification here; our goal is to make this notion precise.

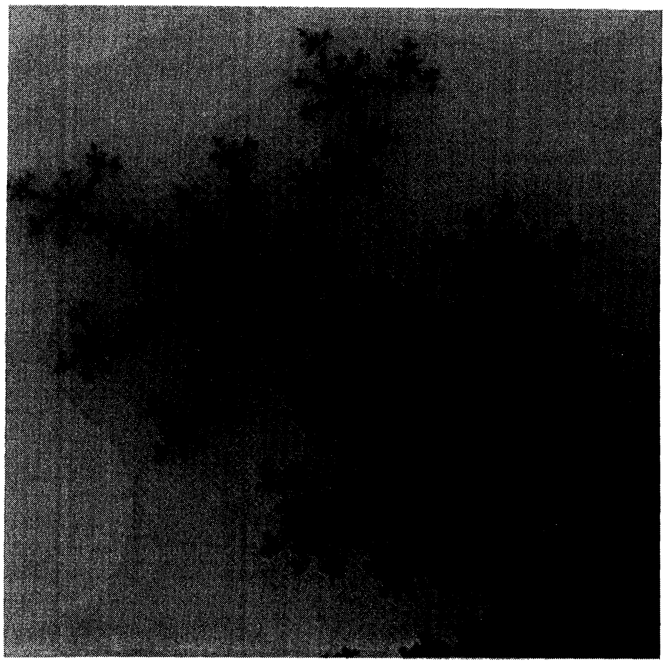


Figure 3. The 3/7 bulb.

As an additional disclaimer, this folk theorem is only about 80% true using the Euclidean notion of "smallness" or Lebesgue measure. We provide a somewhat different framework in which this result is always true.

There is more to the story of interplay between the geometry of the Mandelbrot set and the corresponding dynamics. In Figure 4, we display the $1/2$ and $1/3$ bulbs. The $1/2$ bulb is the large bulb to the left; the $1/3$ bulb is the topmost bulb. In between these two bulbs are infinitely many smaller bulbs, but the largest we recognize as the $2/5$ bulb. Now note that $2/5$ can be obtained from $1/2$ and $1/3$ by "Farey addition":

$$\frac{1}{2} \oplus \frac{1}{3} = \frac{2}{5}.$$

As a second example, note that

$$\frac{2}{5} \oplus \frac{1}{3} = \frac{3}{8}$$

and that the $3/8$ bulb is the largest between the $2/5$ and $1/3$ bulbs; see Figure 5.

That is, to obtain the largest bulb between two given bulbs (in a particular ordering), we simply add the corresponding fractions just the way we always wanted to add them, namely by adding the numerators and adding the denominators. This is the second of the folk theorems we want to discuss. In particular, it follows that the size of bulbs is determined by the Farey tree, as we show in Section 6.

Figures 4 and 5 represent the beginning of a very special sequence of p/q bulbs in the Mandelbrot set

$$\frac{1}{2}, \frac{1}{3}, \frac{2}{5}, \frac{3}{8}, \frac{5}{13}, \ldots$$

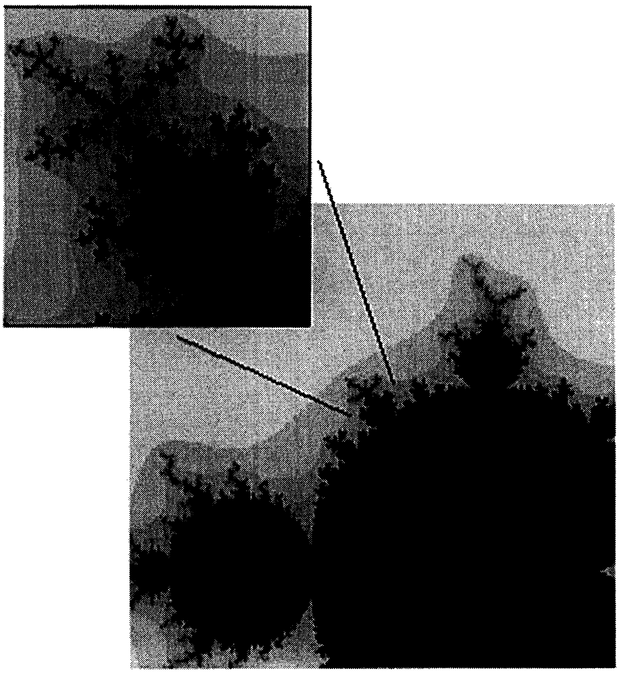


Figure 4. $\frac{1}{2} \oplus \frac{1}{3} = \frac{2}{5}$.

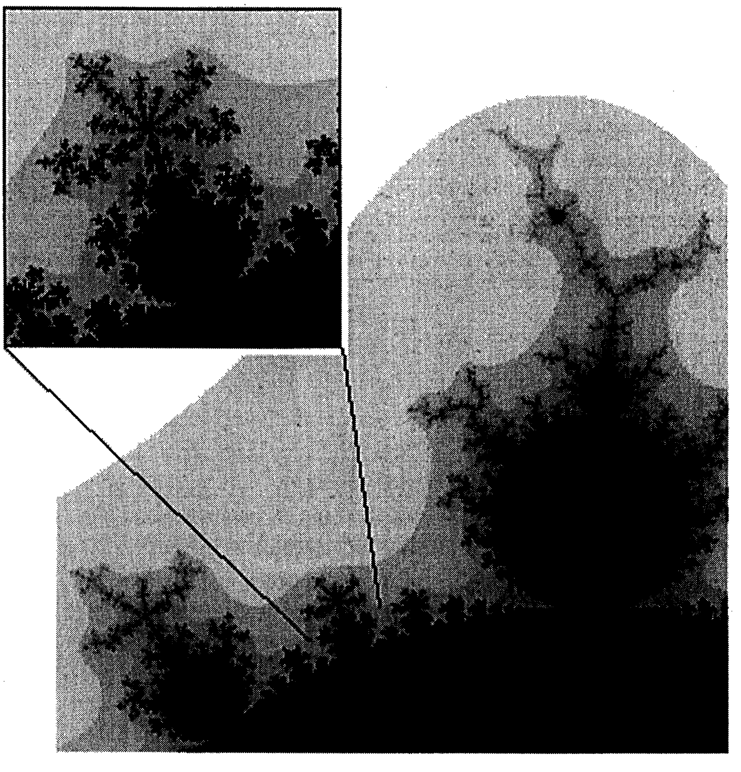


Figure 5. $\frac{2}{5} \oplus \frac{1}{3} = \frac{3}{8}$.

whose numerators and denominators correspond to the Fibonacci sequence. We discuss this connection in more detail in Section 8.

While we do not give complete proofs of each of these folk theorems, we do indicate some of the combinatorial arguments involved in making the statements precise. For more folk theorems and complete proofs, see [5].

2. THE FAREY TREE. Before discussing the Mandelbrot set, we recall a few facts about the *Farey tree*, which is a tree containing all of the rationals between 0 and 1. At each stage of its construction, the Farey tree consists of a finite list of rationals. Adjacent rationals in this list are called *Farey neighbors*. The inductive step in the construction of the tree is: Each pair of Farey neighbors produces a *Farey child*, which is the rational between the two whose denominator is the smallest. Naturally, the rationals that produce a Farey child are called its *Farey parents*.

One of the most intriguing features of the Farey tree is that we obtain Farey children by Farey addition. That is, the fraction between the Farey neighbors α/β and γ/δ is given by

$$\frac{\alpha}{\beta} \oplus \frac{\gamma}{\delta} = \frac{\alpha + \gamma}{\beta + \delta}.$$

So, to obtain the fraction between two Farey neighbors whose denominator is the smallest, we simply add the numerators and add the denominators of the parents to obtain the child. For a proof that this yields the fraction between the parents with smallest denominator, we refer to [8].

We begin the construction of the tree with the pair of rationals 0 and 1, which we write as $0/1$ and $1/1$. Their child is $1/2$, so the second stage of the construction gives the list

$$\frac{0}{1} \quad \frac{1}{2} \quad \frac{1}{1}.$$

At the next stage we obtain two new Farey children

$$\frac{0}{1} \quad \frac{1}{3} \quad \frac{1}{2} \quad \frac{2}{3} \quad \frac{1}{1}.$$

At generation four we find

$$\frac{0}{1} \quad \frac{1}{4} \quad \frac{1}{3} \quad \frac{2}{5} \quad \frac{1}{2} \quad \frac{3}{5} \quad \frac{2}{3} \quad \frac{3}{4} \quad \frac{1}{1}.$$

The Farey tree contains all rationals; see [8] or [9] for more details.

One other fact that we use is that α/β and γ/δ are Farey neighbors if and only if $\alpha\delta - \gamma\beta = \pm 1$. Consequently, we have

$$\left| \frac{\alpha}{\beta} - \frac{\gamma}{\delta} \right| = \frac{1}{\beta\delta}. \tag{1}$$

This equality is easily proved by induction.

3. THE MANDELBROT SET. The Mandelbrot set is

$$\mathscr{M} = \{c | Q_c^n(0) \text{ is bounded}\}$$

for $Q_c(z) = z^2 + c$. Thus $\mathscr{M}$ gives a picture of those c-values for which the orbit of 0 under Q_c does not tend to ∞.

The visible bulbs in $\mathscr{M}$ correspond to c-values for which Q_c has an attracting cycle of some given period. For example, the main central cardioid in $\mathscr{M}$ consists of c-values for which Q_c has an attracting fixed point. This can be seen by solving for the fixed points $(z^2 + c = z)$ that are *attracting*: $|Q_c'(z)| = |2z| < 1$. Solving these equations simultaneously, we see that the boundary of this region is given by $c = z - z^2$, where $z = \frac{1}{2}e^{2\pi i \theta}$. That is,

$$c(\theta) = \frac{1}{2}e^{2\pi i \theta} - \frac{1}{4}e^{4\pi i \theta}$$

parametrizes the boundary of the cardioid with $0 \leq \theta \leq 1$. At $c(\theta)$, $Q_{c(\theta)}$ has a fixed point that is neutral; the derivative of $Q_{c(\theta)}$ at this fixed point is $e^{2\pi i \theta}$.

For each rational value of θ, there is a bulb tangent to the main cardioid at $c(\theta)$. For c-values in the bulb attached to the cardioid at $c(p/q)$, Q_c has an attracting cycle of period q. We call this bulb the p/q bulb attached to the main cardioid and denote it by $B_{p/q}$.

It is known that, as c passes from the main cardioid, through $c(p/q)$, and into $B_{p/q}$, Q_c undergoes a p/q-bifurcation. By this we mean: when c lies in the main cardioid near $c(p/q)$, Q_c has an attracting fixed point with a nearby repelling cycle of period q. At $c(p/q)$ the attracting fixed point and repelling cycle merge to produce a neutral fixed point with derivative $e^{2\pi i p/q}$. When c lies in $B_{p/q}$, Q_c now has an attracting cycle of period q and a repelling fixed point.

When $c = c(p/q)$, the local (linearized) dynamics are given by rotation through angle $2\pi(p/q)$. As a consequence, for nearby $c \in B_{p/q}$, the attracting cycle rotates about the repelling fixed point by jumping approximately $2\pi(p/q)$ radians at each iteration. For more details see [**2**].

4. ANGLE DOUBLING MOD 1. To prepare to use the fundamental results of Douady and Hubbard [**6**] regarding the Mandelbrot set we digress to recall some facts about the *doubling function*, which is defined on the circle considered as the reals modulo one and is given by $D(\theta) = 2\theta \bmod 1$.

Fact 1: The angle θ is periodic under D if and only if θ is a rational of the form p/q (in lowest terms) with q odd.

For example, the D-orbit of $1/3$ is

$$\frac{1}{3} \to \frac{2}{3} \to \frac{1}{3} \to \cdots,$$

which has period 2. The rational $1/7$ has period 3 under doubling:

$$\frac{1}{7} \to \frac{2}{7} \to \frac{4}{7} \to \frac{1}{7} \to \cdots,$$

while $1/5$ has period 4:

$$\frac{1}{5} \to \frac{2}{5} \to \frac{4}{5} \to \frac{3}{5} \to \frac{1}{5} \to \cdots.$$

The rationals with even denominator are eventually periodic but not periodic. For example, $1/6$ lies on an eventual 2-cycle

$$\frac{1}{6} \to \frac{1}{3} \to \frac{2}{3} \to \frac{1}{3} \to \cdots,$$

and $1/8$ is eventually fixed:

$$\frac{1}{8} \to \frac{1}{4} \to \frac{1}{2} \to 1 \to 1 \to \cdots.$$

A second important fact about doubling is that we can read off the binary expansion of θ by noting the *itinerary* of θ in the circle relative to D. To define the itinerary, we denote the upper semicircle $0 \leq \theta < 1/2$ by I_0 and the lower semicircle $1/2 \leq \theta < 1$ by I_1. Given θ, we attach an infinite string of 0's and 1's to θ as follows: The itinerary of θ is $B(\theta) = (s_0 s_1 s_2 \dots)$, where s_j is either 0 or 1: $s_j = 0$ if $D^j(\theta) \in I_0$, and $s_j = 1$ if $D^j(0) \in I_1$. That is, we simply watch the orbit of θ in the circle under doubling and assign 0 or 1 to the itinerary whenever $D^j(\theta)$ lands in the arc I_0 or I_1.

Fact 2: The itinerary $B(\theta)$ is the binary expansion of θ.

For example, if $\theta = 1/3$, then $\theta \in I_0$, while $D(\theta) \in I_1$ and $D^2(\theta) = \theta$. Hence $B(1/3)$ is the repeating sequence $\overline{01}$, which of course is the binary expansion of $1/3$. Similarly, $B(1/7) = \overline{001}$ while $B(1/5) = \overline{0011}$.

5. EXTERNAL RAYS. In order to make precise the folk theorems mentioned in the introduction, we recall some beautiful results of Douady and Hubbard [7] concerning the external rays of the Mandelbrot set.

Let $E = \{z \mid |z| > 1\}$ denote the exterior of the unit circle in the plane. According to Douady and Hubbard, there is a unique analytic isomorphism Φ that maps E to the exterior of the Mandelbrot set. The mapping Φ takes positive reals to positive reals. This mapping is the uniformization of the exterior of the Mandelbrot set, or the exterior Riemann map.

The importance of Φ stems from the fact that the image under Φ of the straight rays $\theta =$ constant in E have dynamical significance. In the Mandelbrot set, we define the *external ray with external angle* θ_0 to be the Φ-image of $\theta = \theta_0$. It is known that an external ray whose angle θ_0 is rational actually "lands" on $\mathscr{M}$. That is $\lim_{r \to 1} \Phi(re^{2\pi i \theta_0})$ exists and is a unique point on the boundary of $\mathscr{M}$. This c-value is called the *landing point* of the ray with angle θ_0.

For example, the ray with angle 0 lies on the real axis and lands on $\mathscr{M}$ at the cusp of the main cardioid, namely $c = 1/4$. Also, the ray with angle $1/2$ lies on the negative real axis and lands on $\mathscr{M}$ at the tip of the "tail" of $\mathscr{M}$, which can be shown to be $c = -2$.

Consider now the interior of $\mathscr{M}$. The interior consists of infinitely many simply connected regions. A *bulb* of $\mathscr{M}$ is a component of the interior of $\mathscr{M}$ in which each c-value corresponds to a quadratic function that admits an attracting cycle. The period of this cycle is constant over each bulb. In many cases, a bulb is attached to a component of lower period at a unique point called the *root point* of the component.

An important result of Douady and Hubbard is:

Theorem 1. *Suppose a bulb B consists of c-values for which the quadratic map has an attracting q-cycle. Then the root point of this bulb is the landing point of exactly 2 rays, and the angles of each of these rays have period q under doubling.*

Thus, the angles of the external rays of $\mathscr{M}$ determine the ordering of the bulbs in $\mathscr{M}$. For example, the large bulb directly to the left of the main cardioid is the

1/2 bulb, so two rays with period 2 under doubling must land there. Now the only angles with period 2 under doubling are 1/3 and 2/3, so these are the angles of the rays that land at the root point of $B_{1/2}$.

Now consider the 1/3 bulb atop the main cardioid. This bulb lies "between" the rays 0 and 1/3. There are only two angles between 0 and 1/3 that have period 3 under doubling, namely 1/7 and 2/7, so these are the rays that land at the root point of $B_{1/3}$.

The 2/5 bulb lies between the 1/3 and 1/2 bulbs. Hence the rays that land at $c(2/5)$ must have period 5 under doubling and lie between 2/7 and 1/3. The only angles that have this property are 9/31 and 10/31, so these rays must land at $c(2/5)$; see Figure 6.

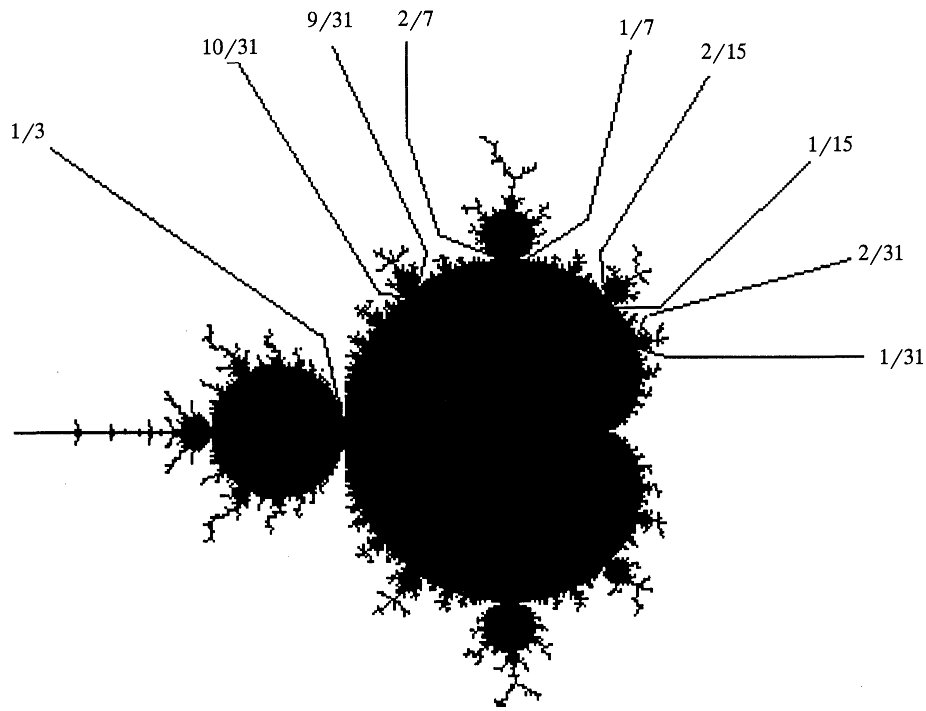


Figure 6. Rays landing on the Mandelbrot set.

These ideas allow us to measure the "largeness" or "smallness" of portions of the Mandelbrot set. Suppose we have two rays with angles θ_- and θ_+ that both land at a point c_* in the boundary of $\mathscr{M}$.

Then, by the isomorphism Φ, all rays with angles between θ_- and θ_+ must approach the component of $M - \{c_*\}$ cut off by θ_- and θ_+. (It is not known that all such rays actually land on $\mathscr{M}$—indeed, this is the major open conjecture about $\mathscr{M}$.) Thus it is natural to measure the size of this portion of $\mathscr{M}$ by the length of the interval $[\theta_-, \theta_+]$.

The root point of the p/q bulb of $\mathscr{M}$ divides $\mathscr{M}$ into two sets. The component containing the p/q bulb is called the p/q *limb*. We can then measure the size of the p/q limb if we know the external rays that land on the root point of the p/q bulb. We compute these rays in the next section.

6. RAYS LANDING ON THE p/q BULB. In order to make the notion of "large" or "small" precise in the statement of the folk theorems, we need a way to determine the angles of the rays landing at the root point of $B_{p/q}$. We denote the angles of these two rays in binary by $\overline{l_{\pm}(p/q)}$, where $\overline{l_{-}(p/q)} < \overline{l_{+}(p/q)}$. We call $\overline{l_{-}(p/q)}$ the *lower angle* of $B_{p/q}$ and $\overline{l_{+}(p/q)}$ the *upper angle*.

As we will see, $l_{\pm}(p/q)$ is a string of q digits (0 or 1) and so $\overline{l_{\pm}(p/q)}$ denotes the infinite repeating sequence whose basic block is $l_{\pm}(p/q)$. Douady and Hubbard [**6**] have a geometric method involving Julia sets to determine these angles. Our method is more combinatorial and resembles algorithms due to Atela [**1**], LaVaurs [**10**], and Lau and Schleicher [**11**].

To describe this algorithm, let $R_{p/q}$ denote rotation of the unit circle through p/q turns, i.e.,

$$R_{p/q}(\theta) = e^{2\pi i(\theta + p/q)}.$$

We consider the itineraries of points in the unit circle under R using two different partitions of the circle.

The *lower partition* of the circle is defined as follows. Let $I_0^- = \{\theta | 0 < \theta \leq 1 - p/q\}$ and $I_1^- = \{\theta | 1 - p/q < \theta \leq 1\}$. The boundary point 0 belongs to I_1^- and $-p/q = 1 - p/q$ belongs to I_0^-. We then define $\overline{s_{-}(p/q)}$ to be the itinerary of p/q under $R_{p/q}$ relative to this partition. We call the basic repeating block of this itinerary, $s_{-}(p/q)$, the *lower itinerary of p/q*. That is, $s_{-}(p/q) = s_1 \dots s_q$ where s_j is either 0 or 1 and the digit s_j is 0 if and only if $R_{p/q}^{j-1}(p/q) \in I_0^-$. Otherwise, $s_j = 1$.

For example, $s_{-}(1/3) = 001$ since

$$I_0^- = (0, 2/3], \qquad I_1^- = (2/3, 1],$$

and the orbit $\frac{1}{3} \to \frac{2}{3} \to 1 \to \frac{1}{3} \to \cdots$ lies in I_0^-, I_0^-, I_1^-, respectively.

Similarly, $s_{-}(2/5) = 01001$ since

$$I_0^- = (0, 3/5], \qquad I_1^- = (3/5, 1],$$

and the orbit is $\frac{2}{5} \to \frac{4}{5} \to \frac{1}{5} \to \frac{3}{5} \to 0 \to \frac{2}{5} \to \cdots$.

We also define the *upper partition* I_0^+ and I_1^+ as follows:

$$I_0^+ = [0, 1 - p/q), \qquad I_1^+ = [1 - p/q, 1).$$

The *upper itinerary of p/q*, $s_{+}(p/q)$, is then the repeating block of the itinerary of p/q relative to this partition. Note that I_0^+ and I_1^+ differ from I_0^- and I_1^- only at the endpoints.

For example, $s_{+}(1/3) = 010$ since the orbit is $\frac{1}{3} \to \frac{2}{3} \to 0 \cdots$ and

$$I_0^+ = [0, 2/3), \qquad I_1^+ = [2/3, 1).$$

This orbit starts in I_0^+, hops to I_1^+, and then returns to I_0^+ before cycling. For 2/5, we have

$$I_0^+ = [0, 3/5), \qquad I_1^+ = [3/5, 1)$$

and $s_{+}(2/5) = 01010$.

The following theorem provides an algorithm for computing the angles of rays landing at $c(p/q)$. For a proof, we refer to [**5**] and [**6**].

Theorem 2. *The rays $\overline{l_{\pm}(p/q)}$ landing at the root point $c(p/q)$ of the p/q bulb are given by $\overline{s_{-}(p/q)}$ and $\overline{s_{+}(p/q)}$.*

Note that $s_{\pm}(p/q)$ differ only in their last two digits (provided $q \geq 2$). Indeed we may write

$$s_{-}(p/q) = s_1 \dots s_{q-2} 0\, 1$$
$$s_{+}(p/q) = s_1 \dots s_{q-2} 1\, 0$$

The reason for this is that the upper and lower itineraries are the same except at $R_{p/q}^{q-2}(p/q) = -p/q$ and $R_{p/q}^{q-1}(p/q) = 0$, which form the endpoints of the two partitions of the circle.

We now define the *size of the p/q limb* to be the length of the interval $[s_{-}(p/q), s_{+}(p/q)]$. That is, the size of the p/q limb is given by the number of external rays that approach this limb. We may compute size of these bulbs explicitly by using the fact that $s_{\pm}(p/q)$ differ only in the last two digits.

Theorem 3. *The size of the p/q limb is $1/(2^q - 1)$. That is*

$$\overline{s_{+}(p/q)} - \overline{s_{-}(p/q)} = \frac{1}{2^q - 1}. \tag{2}$$

Proof: We write the binary expansion of the difference in the form

$$\begin{aligned} \overline{s_{+}(p/q)} - \overline{s_{-}(p/q)} &= \frac{1}{2^{q-1}} + \frac{1}{2^{2q-1}} + \frac{1}{2^{3q-1}} \\ &\quad + \cdots - \left(\frac{1}{2^q} + \frac{1}{2^{2q}} + \frac{1}{2^{3q}} + \cdots \right) \\ &= \frac{1}{2^{q-1}} \cdot \frac{2^q}{2^q - 1} - \frac{1}{2^q} \cdot \frac{2^q}{2^q - 1} = \frac{1}{2^q - 1}. \end{aligned}$$ ∎

As we see in Figure 7, the visual size of the bulbs does indeed correspond to the size as defined above.

7. THE SIZE OF LIMBS AND THE FAREY TREE. In this section we relate the size of a p/q limb to the size of the limbs corresponding to the Farey parents of p/q. The following proposition relates the upper and lower itineraries of p/q and its Farey parents.

Proposition 1. *Suppose α/β and γ/δ are the Farey parents of p/q and that $0 < \alpha/\beta < \gamma/\delta < 1$. Then the lower itinerary $s_{-}(p/q)$ consists of the first q digits of the upper angle $\overline{s_{+}(\alpha/\beta)}$ of the smaller parent, and the upper itinerary $s_{+}(p/q)$ consists of the first q digits of the lower angle $\overline{s_{-}(\gamma/\delta)}$ of the larger parent.*

Proof: We consider only $s_{+}(p/q)$; the proof for $s_{-}(p/q)$ is similar.

From (1), we have

$$\frac{\gamma}{\delta} - \frac{p}{q} = \frac{1}{q\delta}.$$

Consider the orbits of p/q and γ/δ relative to the respective rotations $R_{p/q}$ and $R_{\gamma/\delta}$. Since γ/δ rotates faster than p/q, the distance between these orbits advances by $1/q\delta$ at each iteration. We thus have

$$R_{\gamma/\delta}^{j}(\gamma/\delta) - R_{p/q}^{j}(p/q) = \frac{j+1}{q\delta}.$$

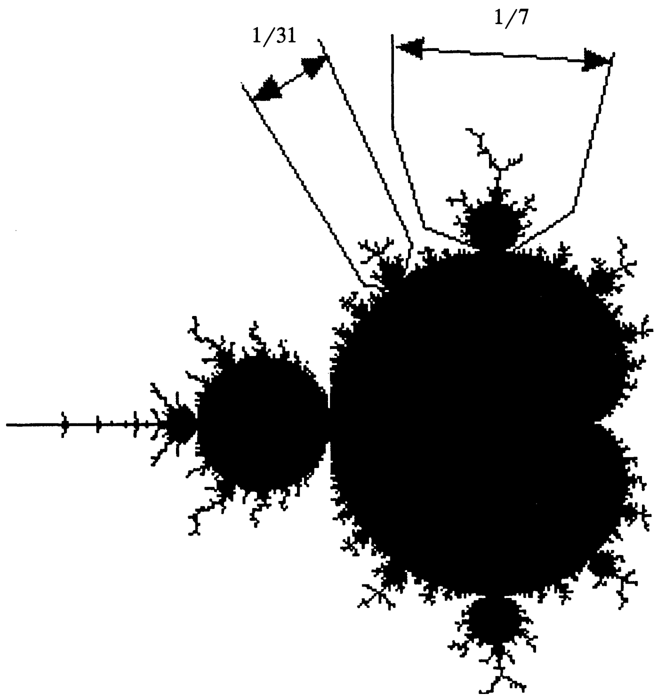


Figure 7. Size of the 2/5 and 1/3 limbs of $\mathscr{M}$.

It follows that $R^j_{p/q}(p/q)$ lies within $1/\delta$ units of $R^j_{\gamma/\delta}(\gamma/\delta)$ provided $j < q - 1$. Since points on the orbit of γ/δ under $R_{\gamma/\delta}$ lie exactly $1/\delta$ units apart on the circle, it follows that the first $q - 1$ entries in the itineraries of p/q and γ/δ are the same, provided we choose the lower itinerary for γ/δ and the upper itinerary for p/q. The reason for this is that the orbit of γ/δ lies ahead of that of p/q in the counterclockwise direction, but by no more than $1/\delta$ units. Choosing the upper itinerary for p/q and the lower for γ/δ forces the corresponding digits to be the same.

When $j = q - 1$, we have $R_{p/q}(p/q) = 0$ and

$$R^{q-1}_{\gamma/\delta}(\gamma/\delta) - R^{q-1}_{p/q}(p/q) = \frac{q}{q\delta} = \frac{1}{\delta}.$$

Hence

$$R^{q-1}_{\gamma/\delta}(\gamma/\delta) = \frac{1}{\delta}.$$

Therefore the qth digit in $s_+(p/q)$ is 0 and so is the qth digit of γ/δ, as long as $\gamma/\delta \neq 1$. ■

If one of the Farey parents is 0 or 1, we must modify Proposition 1.

Proposition 2. *Suppose that* 0 *is a Farey parent of* p/q. *Then the* q *digits in the lower itinerary of* p/q *are* $s_-(p/q) = 0\ldots01$. *If* 1 *is a Farey parent of* p/q *then* $s_+(p/q) = 1\ldots10$.

Proof: For $s_-(p/q)$, we first note that, since $0/1$ is a Farey parent, we must have $p = 1$. Thus, $s_-(p/q)$ is given by the itinerary of $1/q$ under counterclockwise rotation by $1/q$ units. We therefore have

$$I_0^- = (0, (q-1)/q], \qquad I_1^- = ((q-1)/q, 1].$$

It follows that the first $q-1$ digits of $s_-(1/q)$ are 0, and the last digit is 1. If a Farey parent is $1/1$, the proof is similar, since in this case $p = q - 1$. ■

We now complete the proof of one of the folk theorems mentioned in the introduction.

Theorem 4. *Suppose α/β and γ/δ are the Farey parents of p/q and that $0 \le \alpha/\beta < \gamma/\delta \le 1$. Then the size of the p/q limb is larger than the size of any other limb between the α/β and γ/δ limbs.*

Proof: Assume first that neither parent is 0 or 1. Propositions 1 and 2 ensure that $\overline{s_-(p/q)}$ and $\overline{s_+(\alpha/\beta)}$ agree in their first q digits. Using these binary representations, we have

$$\overline{s_-(p/q)} - \overline{s_+(\alpha/\beta)} \le \frac{1}{2^q}.$$

Similarly

$$\overline{s_-(\gamma/\delta)} - \overline{s_+(p/q)} \le \frac{1}{2^q}.$$

This implies that the arc of rays between the p/q limb and either of its parents' limbs has length no larger than $1/2^q$. Thus any limb between them has size smaller than $1/2^q$.

From (2), we know that

$$\overline{s_+(p/q)} - \overline{s_-(p/q)} = \frac{1}{2^q - 1}.$$

As this quantity is larger than $1/2^q$, it follows that the p/q limb attracts the largest number of rays between its two parents.

If one of the parents of $1/q$ is 0, then the size of the $1/q$ bulb is again $1/(2^q - 1)$, while the gap between 0 and $\overline{s_-(p/q)} = \overline{0 \dots 01}$ is also $1/(2^q - 1)$. But then any limb between the $1/q$ limb and the cusp of the cardioid must have size strictly smaller than $1/(2^q - 1)$, again showing that the $1/q$ limb is the largest. The case of Farey parent 1 is handled similarly. ■

8. THE FIBONACCI SEQUENCE. Theorem 4 shows that the Fibonacci sequence appears in the Mandelbrot set. As we have seen in Figures 4 and 5, the largest bulb between the $1/2$ and $1/3$ bulb is the $2/5$ bulb, and the largest between the $1/3$ and $2/5$ bulbs is the $3/8$ bulb. This progression continues, with the numerators (and denominators) forming the Fibonacci sequence. For example, we next have

$$\frac{2}{5} \oplus \frac{3}{8} = \frac{5}{13}.$$

The corresponding bulbs are shown in Figure 8.

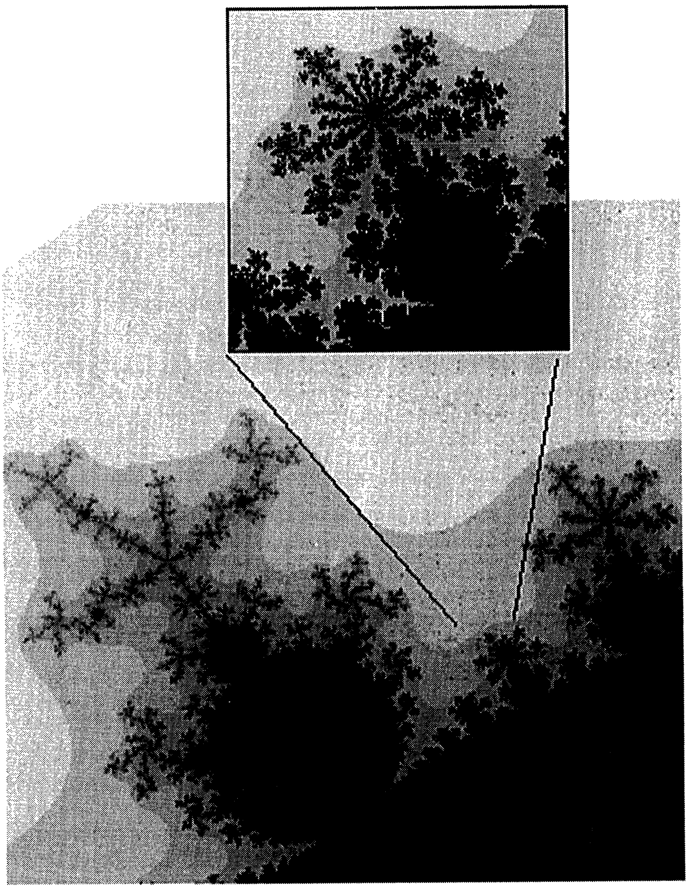


Figure 8. $\frac{2}{5} \oplus \frac{3}{8} = \frac{5}{13}$.

This sequence of bulbs actually converges to a single point on the boundary of the main cardioid. At this particular c-value, Q_c is known to have a fixed point z_0 with $Q_c'(z_0) = e^{2\pi i\theta}$, where θ is related to the golden ratio and hence is *highly irrational.* The dynamics of complex functions near such fixed points is the subject of the Fields' Medal work of J.-C. Yoccoz **[12]**.

9. CONCLUSION. The technique of measuring the size of certain portions of the Mandelbrot set by the length of the interval of rays that land on that portion provides justification for other folk theorems involving the size of $\mathscr{M}$. For example, this technique is used to identify the p/q bulb using the "lengths" of the spokes in its antenna. Once we know these rays, we can easily compute the lengths of the various spokes.

For example, it can be shown that the two rays that land at the junction point of the antenna adjacent to the principal spoke are given by $s_-\overline{s_+}$ and $s_+\overline{s_-}$, where we have dropped the p/q for clarity. These two rays are therefore given by preperiodic binary sequences that begin to repeat only after the qth entry. Thus, the vast majority of rays that land on the p/q limb actually approach the spokes of the antenna. For we have the following ordering of the rays landing on the p/q bulb:

$$\overline{s_-} < s_-\overline{s_+} < s_+\overline{s_-} < \overline{s_+}.$$

It is easy to check that the length of the arc of rays approaching the antenna between $s_-\overline{s_+}$ and $s_+\overline{s_-}$ is

$$\frac{1}{2^{q-1}} - \frac{2}{2^q(2^{q-1})}.$$

This number is much larger (for large q) than the length of the arc between $\overline{s_-}$ and $s_-\overline{s_+}$ or between $\overline{s_+}$ and $s_+\overline{s_-}$, each of which has length

$$\frac{1}{2^q(2^{q-1})}.$$

We can also use the two rays separating the principal spoke from the rest of the antenna to determine a list of the q rays that land on the junction point. Then we can determine that the shortest is located p/q turns in the counterclockwise direction from the principal spoke. See [**5**] for details.

REFERENCES

1. P. Atela, Bifurcations of Dynamic Rays in Complex Polynomials of Degree Two, *Ergod. Th. & Dynam. Sys.* **12** (1991) 401–423.
2. B. Branner, The Mandelbrot Set, in *Chaos and Fractals: The Mathematics Behind the Computer Graphics*. Amer. Math. Soc. (1989), pp. 75–106.
3. P. Blanchard, Complex Analytic Dynamics on the Riemann Sphere, *Bull. Amer. Math. Soc.* **2** (1984) 85–141.
4. R. L. Devaney, The Fractal Geometry of the Mandelbrot Set: II. How to Add and How to Count, *Fractals* **3** (1995) 629–640. See also `http://math.bu.edu/DYSYS/FRACGEOM2/FRACGEOM2.html`
5. R. L. Devaney, The Fractal Geometry of the Mandelbrot Set III; Geometry of the Bulbs, preprint.
6. A. Douady and J. Hubbard, Étude Dynamique des Polynôuome Complexes, *Publications Mathematiques d'Orsay* (1984).
7. A. Douady and J. Hubbard, Itération des Polynôuomes quadratiques complexes, *C. R. Acad. Sci. Paris Sér. I Math.* **294** (1982) 123–126.
8. J. Farey, On a curious property of vulgar fractions, *Phil. Mag. J. London* **47** (1816) 385–386.
9. L. Goldberg and C. Tresser, Rotation orbits and the Farey tree, *Ergod. Thy. & Dynam. Sys.* **16** (1996) 1011–1029.
10. P. LaVaurs, Une Description Combinatoire de l'involution definie par M sur les rationelles a denominateur impaire, *C. R. Acad. Sci. Paris Sér. I Math.* **303** (1986) 143–146.
11. E. Lau and D. Schleicher, Internal Addresses in the Mandelbrot Set and Irreducibility of Polynomials, *SUNY Stony Brook Institute for Mathematical Sciences* Preprint #1994–19.
12. J.-C. Yoccoz, Thórème de Siegel, nombres de Brjuno, et polynôuomes quadratiques, *Astérisque* **231** (1995) 3–88.

ROBERT L. DEVANEY received his Ph.D. at the University of California, Berkeley in 1973. He has taught at Northwestern, Tufts, and the University of Maryland before coming to Boston University in 1980. In 1995 he was awarded the Deborah and Franklin Tepper Haimo Award for Distinguished University Teaching by the MAA. When he is not trying to figure out $x^2 + c$, he can usually be found either sailing the waters off New England or humming along at the nearest opera house.
Boston University, Boston, MA 02215
bob@bu.edu

Existence Proofs

Fred Richman

[If] a proof convinces you that there is a root of an equation (without giving you any idea *where*)—how do you know that you understand the proposition that there is a root? Ludwig Wittgenstein

The proposition that mathematics is grounded on computation would seem to be quite uncontroversial; the only people I have heard argue against it are mathematicians. By "mathematics" I mean pure mathematics—theorems and proofs. Many pure mathematicians think that they engage in a high art form that is incompatible with strong links to computation, the nerdy province of bookkeepers, statisticians, and calculators. This attitude goes hand in glove with the practically unquestioned acceptance of nonconstructive existence proofs in modern mathematics.

Constructive mathematicians are unsatisfied by nonconstructive existence proofs: proofs that attempt to convince you of the existence of a number, or of some more complicated mathematical object, without giving any method for computing it. The difference between constructive mathematics and classical mathematics is that when a constructive mathematician says there is a number that satisfies a given equation, or has some other property, he has an algorithm in his pocket for computing that number. The pocket of a classical mathematician, who makes the same statement, might contain only a derivation of a contradiction from the assumption that every number fails to have the property.

The quotation from Wittgenstein [**12**, p. 282] at the head of this article suggests that the peculiar nature of such a proof should cause us to reconsider the meaning of the proposition it proves. Did we really understand what was meant by "there is a root" if we can be convinced of its truth by an argument that does not provide a method for finding a root? What are these numbers that exist without our being able to construct them? I am reminded of the Nobel laureate Eugene Wigner's response to the question of whether there are any inherently unknowable laws of physics: he said, "I don't know of any."

I will illustrate the idea of a nonconstructive proof by several examples. The first is of a theorem that admits a celebrated constructive proof (the Euclidean algorithm). Many textbooks give both proofs, but the constructive one is usually presented as a method of computation rather than a proof.

Theorem 1. *There exist integers s and t such that* $437s + 323t$ *is positive and divides* 437 *and* 323.

Of course the numbers 437 and 323 are not special; I choose them to make sure we see immediately which are the constants and which are the variables. It follows immediately from the theorem that the number $437s + 323t$ is the greatest common divisor of 437 and 323. Here is a nonconstructive proof of the theorem.

Proof: Consider the set of positive integers

$$S = \{d : d > 0 \text{ and } d = 437s + 323t \text{ for some } s \text{ and } t\}.$$

The set S is nonempty because 437 and 323 are clearly in it. Therefore, by what is often called the "well-ordering principle," there is a least element d_0 of S. As $d_0 \in S$ we can write $d_0 = 437s_0 + 323t_0$. The division algorithm enables us to write $437 = qd_0 + r$, where $0 \leq r < d_0$. If $r > 0$, then $r = 437(1 - qs_0) + 323(-qt_0)$ is in S. But d_0 is the smallest element of S, so $r = 0$. Thus d_0 divides 437; similarly d_0 divides 323. ■

That was a proof in the spirit of the Wittgenstein quotation. What are these integers s and t that we have shown to exist? We have not been given a clue as to how to find them. They were constructed by choosing the smallest element of the set S. But how do we find that smallest element? What is the basis for the well-ordering principle?

A proof of the well-ordering principle, as applied to a set S of positive integers that contains 323, might go as follows. If $1 \in S$, then 1 is the smallest element of S. If $1 \notin S$, but $2 \in S$, then 2 is the smallest element of S. If $1 \notin S$ and $2 \notin S$, but $3 \in S$, then 3 is the smallest element of S. We can write this as a computer program as follows: for $i = 1$ to 323 do if $i \in S$ return i.

What does this proof of the well-ordering principle prove? It proves that a nonempty detachable subset of the positive integers has a least element. A subset S of a set X is called *detachable* if you can tell (there is an algorithm for telling) whether or not any given element of X is in S. The problem with the set S in the proof of Theorem 1 is that we have not established that it is detachable; for example, how do we decide whether or not $1 \in S$? In fact S is detachable, but to prove that we usually invoke Theorem 1!

A constructive proof of Theorem 1 might go like this. Consider the following table.

437	1	0
323	0	1
114	1	−1
95	−2	3
19	3	−4

Each row represents values of d, s, and t such that $d = 437s + 323t$. This is clear for the first two rows. Each subsequent row R_{n+1} is computed from the previous two rows R_{n-1} and R_n by setting $R_{n+1} = R_{n-1} - m_n R_n$. We choose the m_n so as to make the first entry of R_{n+1} positive, and as small as possible. The first entries of the rows must decrease, unless the first entry of R_n divides the first entry of R_{n-1}, in which case we stop. The equation $d = 437s + 323t$ is inherited by R_{n+1} from R_n and R_{n-1}. Moreover, as $R_{n-1} = m_n R_n + R_{n+1}$, any number that divides the first entries of two consecutive rows, divides the first entry of the row before them. So 19 divides all the numbers above it; in particular, 437 and 323.

Errett Bishop, the mathematician most responsible for the recent renaissance of constructive mathematics, formulated four principles of constructive mathematics in [**2**]:

(A) *Mathematics is common sense.*
(B) *Do not ask whether a statement is true until you know what it means.*
(C) *A proof is any completely convincing argument.*
(D) *Meaningful distinctions deserve to be maintained.*

Constructivists think that a proof of the existence of a mathematical object should tell you how to construct that object; this follows from their belief that other interpretations of the phrase "there exists," in a mathematical context, are either incomprehensible, or can be formulated in more descriptive ways (principles B and D).

These are controversial, even revolutionary, ideas. Constructivists want to make fundamental changes in the way we view mathematics; they want to change the rules by which the game of mathematics is played. But most people aren't interested in changing the rules. For one reason, most people like the rules as they are. In fact, successful mathematicians have a vested interest in keeping the rules as they are. Why should a champion chess player be interested in changing the rules of chess? Another reason is that, after all, aren't the present rules of mathematics correct? How can there be any serious alternatives?

Constructive mathematics is not just an idea but a substantial body of results. In **[1]** Bishop developed much of analysis along constructive lines. This classic book has been revised and extended **[3]**. A corresponding constructive development of algebra was carried out in **[9]**. For expository articles on constructive mathematics see **[4]**, **[5]**, **[8]**, **[10]**, and **[11]**.

Let's look at another example: consider the decimal expansion

$$\pi = 3.14159265358979323846264338327 95\ldots.$$

This decimal expansion suits our purposes because it is a familiar example of a computable infinite sequence, and very little is known about it. The theorem I want to consider says that

Theorem 2. *There is a digit that appears infinitely often in the decimal expansion of* π.

How can we establish such a theorem in light of the fact that so little is known about the decimal expansion of π? As you may have already realized, the proof that I have in mind gives you no idea as to which digit appears infinitely often. It is a genuine indirect proof, as opposed to the usually cited examples of proof by contradiction—proofs that $\sqrt{2}$ is not rational, or that the number of primes is not finite—where the very meaning of the theorem requires that a contradiction be derived.

Let's look at a proof of this theorem.

Proof: Suppose each digit occurs only a finite number of times in the decimal expansion of π: so 0 occurs n_0 times, 1 occurs n_1, times, etc. Then compute

$$n_0 + n_1 + \cdots + n_9 + 1$$

places in the decimal expansion of π. But there are only $n_0 + n_1 + \cdots + n_9$ digits available to fill up these places, which is absurd, so our original assumption that each digit occurred only finitely many times must be false. ∎

What has been proved? Let P_i denote the proposition that the digit i appears (only) a finite number of times in the decimal expansion of π. Then we have shown that the proposition

$$A = P_0 \text{ and } P_1 \text{ and} \cdots \text{and } P_9$$

leads to a contradiction. That is, we have proved the negation $\neg A$ of the proposition A. What we wanted to show, on the other hand, was that $\neg P_i$ holds for some digit i, that is we wanted to prove the proposition

$$B = \neg P_0 \text{ or } \neg P_1 \text{ or} \cdots \text{or } \neg P_9.$$

According to the usual laws of logic (DeMorgan's law), B is the same as $\neg A$, which we *have* proved. The constructivist grants that $\neg A$ has been proved, but denies that B has been proved. He wants to draw a distinction between B, which asserts the existence of a digit with the property $\neg P$, and $\neg A$, which merely says that it is impossible for all digits to have the property P (*meaningful distinctions deserve to be maintained*). So we see what the rules are that constructivists want changed: no less than the rules of logic.

The controversy over nonconstructive techniques in mathematics goes back at least to the beginning of this century. David Hilbert and L.E.J. Brouwer were the principal participants in this controversy. Brouwer founded the philosophy of mathematics called *intuitionism* [**6**]. Most constructive mathematicians, of whatever school, consider Brouwer to be a spiritual ancestor. Hilbert was the foremost mathematician in Germany, and possibly in the world, in the early twentieth century. Many American mathematicians trace their mathematical lineage to Hilbert because of the German mathematicians who settled in the United States prior to World War II, and the Americans who went to Germany in the early part of the century to study with Hilbert and his students.

Hilbert used nonconstructive techniques to solve a well-known problem concerning the construction of a finite set of polynomials with certain properties. The problem had been solved by P. Gordan, for the case of polynomials in two variables, by explicitly exhibiting the finite set of polynomials. Hilbert solved the general case, but his proof gave no clue how to construct the required polynomials. This appears to be the first use of a nonconstructive proof to establish the existence of mathematical objects that were expected to be constructed explicitly. The reaction of Gordan, perhaps in reference to proofs of the existence of God, was "That's not mathematics, that's theology."

Since then, Hilbert's approach has so dominated mathematical thinking that alternatives are not considered seriously. But Hilbert and Brouwer had one thing in common: they both thought that nonconstructive techniques needed justification. Brouwer thought that the answer was to use only constructive techniques. Hilbert did not want to abandon his nonconstructive techniques; instead, he proposed to show that you couldn't get into trouble using them.

Hilbert's program was to show that if a theorem proved by nonconstructive means predicted the result of a computation, then it would predict the correct result. Thus even if the smallest digit that occurred infinitely often in the decimal expansion of π were just a fiction, we could treat it as reality and still never say anything that was verifiably false. An analogy is the introduction of a square root of -1, which in some sense is simply a fiction, but it helps us to prove things about, and to discover properties of, the numbers that we actually believe in.

Of course the proof that you don't get into trouble using nonconstructive techniques must use only constructive techniques in order to be convincing. Hilbert's program was utterly demolished by Kurt Gödel, who showed in the thirties that not only couldn't you prove such a thing constructively, but you couldn't even prove it using only the nonconstructive techniques that you were attempting to justify. Remarkably, this had no effect on the acceptability of nonconstructive techniques!

My final example of a nonconstructive existence proof comes from the theory of computable functions. That theory was developed to clarify the idea of what it means for a function to be computable. This is not an idea that would occur to a constructivist, for whom computability is part of the intuitive idea of a function: if there exists y such that $f(x) = y$, then we must be able to construct that y if we

are given x. A constructivist can certainly entertain the idea of looking at a restricted class of functions that are computed in a special way, but would be unlikely to call that class "the computable functions."

In the theory of computable functions, a function from the natural numbers $0, 1, 2, \ldots$ to the natural numbers is called *computable* if there exists a computer program to compute it. It is well known that, for all but the most anemic programming languages, this notion is independent of the particular language used. In the standard theory, nonconstructive proofs of the existence of a program are allowed.

It will be convenient to abbreviate the following statement by P_n.

P_n : There are (at least) n consecutive 4's in the decimal expansion of π.

Consider the function f defined by setting $f(n) = 1$ if P_n and $f(n) = 0$ otherwise. Clearly $f(0) = f(1) = 1$. I asked my computer to give me 100 places of π, and I see that there are 4's in places 59 and 60 (if I haven't miscounted), so $f(2) = 1$. But what, for example, is $f(12)$? No one knows; no one even knows of a computation that would resolve this question. If you compute a billion places in the expansion of π you might discover that $f(12) = 1$, but no such computation would tell you that $f(12) = 0$. A constructivist would say that we have not defined f for all n because we have not shown how to compute $f(n)$ in general.

The orthodox view, however, is that not only have we defined f for all n, but that f is computable! To verify the first claim, consider the set

$$G = \{(n, i) : i = 1 \text{ and } P_n, \text{ or } i = 0 \text{ and not } P_n\}.$$

This is the graph of f. To show that f is defined at n means to show that there exists i in the set $\{0, 1\}$ so that (n, i) is in G. It is clear that if $(n, 1)$ is not in G, then $(n, 0)$ is in G, because either statement is equivalent to denying P_n. But this constitutes a nonconstructive proof that there exists i for which (n, i) is in G, as it is impossible that neither $(n, 1)$ nor $(n, 0)$ is in G.

So suppose that f is defined for all n—the constructivist will have to imagine that he can consult an oracle to determine the value of $f(n)$. Now we want to show that there is a program that computes f. This requires a second nonconstructive argument. The gimmick is that we do not have to produce the program; we merely have to show that f cannot be different from each computable function.

Consider the following collection of functions, one for each natural number m:

$$g_m(n) = \begin{cases} 1, & \text{if } n < m \\ 0, & \text{if } n \geq m, \end{cases}$$

together with the function g_∞ which is identically equal to 1. Certainly g_∞ is computable, and g_m is computable for each finite m: the program simply compares n with the fixed number m and returns 1 or 0 as appropriate. Suppose $f(n) = 0$ for some n. Let m be the first place where $f(m) = 0$. Then $f = g_m$ because $f(x) \geq f(y)$ whenever $x \leq y$. Thus if $f \neq g_m$ for each finite m, then $f(n)$ cannot be 0 for any n, so $f = g_\infty$. Therefore f cannot be different from each computable function. That's as far as a constructivist can go, even with an oracle that tells him what $f(n)$ is.

The final (nonconstructive) step in the argument is to apply an infinite version of the DeMorgan's law used in the second example. We have shown that the proposition

$$f \neq g_\infty \text{ and } f \neq g_0 \text{ and } f \neq g_1 \text{ and } \cdots$$

is false. We conclude that the proposition

$$f = g_\infty \text{ or } f = g_0 \text{ or } f = g_1 \text{ or } \cdots$$

is true—if a collection of propositions cannot all be false, then one of them is true. So there exists m such that $f = g_m$, whence f is computable.

I will let Wittgenstein have the last word. Georg Cantor laid the foundation for the theory of transfinite sets upon which twentieth century mathematics is based. Hilbert **[7]**, referring to objections of the intuitionists, said "No one shall drive us out of the paradise which Cantor created for us." Wittgenstein [**13**, p. 103] later wrote in response to this,

> I would say, "I wouldn't dream of trying to drive anyone out of this paradise." I would try to do something quite different: I would try to show you that it is not a paradise—so that you'll leave of your own accord. I would say, "You're welcome to this; just look about you."

REFERENCES

1. Bishop, Errett, *Foundations of constructive analysis*, McGraw-Hill, 1967.
2. ______, Schizophrenia in contemporary mathematics, American Mathematical Society, 1973, in *Errett Bishop: Reflections on him and his research*, AMS Contemporary mathematics series, volume 39, 1985.
3. ______, and Douglas Bridges, *Constructive analysis*, Springer-Verlag, 1985.
4. Bridges, Douglas, and Ray Mines, What is constructive mathematics?, *The Mathematical Intelligencer* **6** (1984) 32–38.
5. Calder, Allan, Constructive mathematics, *Scientific American*, Oct. 1979, 146–171.
6. Heyting, A., *Intuitionism, an introduction*, North-Holland, 1971.
7. Hilbert, David, On the infinite (1925), in *Philosophy of mathematics: selected readings*, Paul Benacerraf and Hilary Putnam (eds.), Cambridge University Press, 1983.
8. Mandelkern, Mark, Brouwerian counterexamples, *Math. Mag.* **62** (1989) 3–27.
9. Mines, Ray, Fred Richman, and Wim Ruitenburg, *A course in constructive algebra*, Springer-Verlag, 1988.
10. Richman, Fred, Meaning and information in constructive mathematics, *Amer. Math. Monthly*, **89** (1982) 385–388.
11. ______, Interview with a constructive mathematician, *Modern Logic* **6** (1996) 247–271.
12. Wittgenstein, Ludwig, *Remarks on the foundations of mathematics*, (1942–1944), edited by G.H. von Wright et al., MIT Press, 1978.
13. ______, *Wittgenstein's lectures on the foundations of mathematics, Cambridge* 1939, edited by Cora Diamond, Cornell University Press, 1976.

FRED RICHMAN has an AB from Princeton University and a PhD from the University of Chicago. After teaching at New Mexico State University for many years, dividing his research time between infinite abelian group theory and constructive mathematics, he worked off and on at TCI Software Research as a developer of Scientific Word and Scientific WorkPlace. He has coauthored texts on modern algebra, mathematics for liberal arts students, constructive algebra, and varieties of constructive mathematics.
Florida Atlantic University, Boca Raton FL 33431
richman@fau.edu

Introduction to Metric-Preserving Functions

Paul Corazza

1. INTRODUCTION. Under what conditions on a function $f:[0,\infty) \to [0,\infty)$ is it the case that for each metric space (X, d), $f \circ d$ is still a metric, and, moreover, d and $f \circ d$ are equivalent metrics?

It is well-known that for any metric d, $d/(1 + d)$ is a (bounded) metric that is equivalent to d. On the other hand, $d/(1 + d^2)$ need not be a metric; see Proposition 2.7. We call $f:[0,\infty) \to [0,\infty)$ *metric-preserving* (respectively, *strongly metric-preserving*) if for all metric spaces (X, d), $f \circ d$ is a metric (respectively, is a metric that is topologically equivalent to d).

Although the first reference in the literature to the notion of metric-preserving functions seems to be [**19**], the first detailed study of these functions was by Sreenivasan in 1947 [**16**]. Kelley's classic text in general topology mentions some of Sreenivasan's results in an exercise [**14**, p. 131]:

Exercise (*Kelley*). Suppose $f:[0,\infty) \to [0,\infty)$ is continuous, nondecreasing, and subadditive ($f(x + y) \leq f(x) + f(y)$ for all x, y). Suppose also that $f^{-1}(0) = \{0\}$. Then f is strongly metric-preserving.

In the past two decades, a significant literature has developed on the subject of metric-preserving functions. The purpose of this paper is to introduce some of the results and techniques of the field to a broader mathematical audience.

We begin our study of metric-preserving functions in the next section, where we build tools to understand these functions and consider some revealing examples. Section 3 examines the important relationship between strongly metric-preserving functions and continuity. In the final section, we survey some of the results on differentiability in the context of metric-preserving functions. Many of the results discussed here have been garnered from papers that have appeared in other languages and in journals unfamiliar to the author; special thanks go to Jozef Doboš for his tremendous help in making so many of these papers available to me. Space constraints prevent me from discussing many avenues of research related to metric-preserving functions that have been pursued by various authors; see [**8**] for an excellent list of references.

An interesting application of metric-preserving functions was discovered by Jůza in 1956, long before the subject had matured [**13**]. It is now well-known that there are complete nowhere discrete metric spaces that have a nested sequence of closed balls with empty intersection (of course the diameters of such balls cannot tend to 0). Jůza observed that the real line could be topologized to obtain such a space, using a metric-preserving function; in particular, he showed that $(\mathbf{R}, f \circ e)$ has the required property if e is the usual metric on $\mathbf{R}$, and f is the metric-preserving function defined by

$$f(x) = \begin{cases} x & \text{if } x \leq 2 \\ 1 + \dfrac{1}{x-1} & \text{if } x > 2. \end{cases} \tag{1.1}$$

We prove that f is metric-preserving in the next section; see **[10]** for technical refinements of this result.

2. METRIC-PRESERVING FUNCTIONS. A metric space is a set X together with a function d: $X \times X \to [0, \infty)$ satisfying the following three conditions:

(M1) For all $x, y \in X$, $d(x, y) = 0$ if and only if $x = y$;
(M2) For all $x, y \in X$, $d(x, y) = d(y, x)$; and
(M3) For all $x, y, z \in X$, $d(x, y) + d(y, z) \geq d(x, z)$.

If a real-valued function f defined on a set $S \subseteq \mathbf{R}$ is metric-preserving, then S must include $[0, \infty)$, its range must lie in $[0, \infty)$, and $f^{-1}(0) = \{0\}$; we call such functions *amenable*. Since the values that an amenable function may have at negative reals have no bearing on whether the function is metric-preserving, we further require that all amenable functions have domain precisely $[0, \infty)$.

The next proposition identifies a basic property of all metric-preserving functions:

Proposition 2.1. *If f is metric-preserving, then f is subadditive.*

Proof: Let $a, b \in [0, \infty)$ and let d be the usual metric on $\mathbf{R}$. Then

$$\begin{aligned} f(a) + f(b) &= (f \circ d)(0, a) + (f \circ d)(a, a + b) \\ &\geq (f \circ d)(0, a + b) = f(a + b). \end{aligned}$$ ∎

Terpe used the subadditivity criterion to show that a fairly broad class of functions is not metric-preserving. Before stating his result, we recall that a function $f : [0, \infty) \to [0, \infty)$ is *convex* on $[0, c]$ if

$$f\left(\frac{x+y}{2}\right) \leq \frac{f(x) + f(y)}{2} = g\left(\frac{x+y}{2}\right) \tag{2.1}$$

whenever $0 \leq x < y < z \leq c$, where the graph of g is the line passing through $(x, f(x)), (y, f(y))$. Moreover, f is *strictly convex* if (2.1) holds when $\leq$ is replaced by $<$.

Corollary 2.2 [18]. *Given $f : [0, \infty) \to [0, \infty)$, suppose that either*

(A) *f is strictly convex on some interval including the origin and $f(0) = 0$, or*
(B) *f is differentiable on (u, ∞) for some $u \geq 0$ and $\lim_{x \to \infty} f'(x) = +\infty$.*

Then f is not metric-preserving.

Proof: For (A), let c be a positive number for which f is strictly convex on $[0, c]$. Then $f(c/2) < f(c)/2$, whence $f(c/2) + f(c/2) < f(c)$, which violates subadditivity.

For (B), assume f is differentiable on (u, ∞), $\lim_{x \to \infty} f'(x) = +\infty$, and f is metric-preserving. Let $x_0 > u$. Because f' tends to $+\infty$, there is an $r > 0$ such that for all $x > r$, $f'(x) > f(x_0)/x_0$. Pick $x_1 > r$ and use the Mean Value Theorem to obtain a $y \in (x_1, x_1 + x_0)$ such that $f'(y) = (f(x_1 + x_0) - f(x_1))/x_0$. It follows that $(f(x_1 + x_0) - f(x_1))/x_0 > f(x_0)/x_0$, which violates subadditivity. ∎

Borsík and Doboš **[1]** give an example of a metric-preserving function f that is differentiable on $(0, \infty)$ and satisfies $\limsup_{x \to \infty} f'(x) = +\infty$, showing that the condition "$\lim_{x \to \infty} f'(x) = +\infty$" in Corollary 2.2(B) is optimal. In the same paper,

the authors extend Corollary 2.2(A); we state their result in Theorem 3.5. The proof makes use of a symmetry between subadditive and convex amenable functions, which is developed in the following exercise:

Exercise 1 [1].

(1) Suppose $f:[0,\infty) \to [0,\infty)$ is subadditive. Show that for all positive integers n, $f(nx) \le nf(x)$ and $f(x/2^n) \ge f(x)/2^n$ whenever $x \ge 0$.
(2) Suppose f is amenable and convex on $[0,c]$. Show that for all positive integers n, $f(x/2^n) \le f(x)/2^n$ whenever $0 \le x \le c$.

While subadditivity is an important necessary condition, the function $x/(1+x^2)$ shows that subadditivity is not sufficient for an amenable function to be metric-preserving. However, adding "nondecreasing" to subadditivity does yield a sufficient condition:

Proposition 2.3. *Suppose f is amenable, subadditive, and nondecreasing. Then f is metric-preserving.*

Proof: Let (X,d) be a metric space; we show $f \circ d$ is a metric. Properties (M1) and (M2) are easy to check. For (M3), let $x, y, z \in X$, and let $a = d(x,y)$, $b = d(y,z)$, and $c = d(x,z)$. It suffices to show that $f(a) + f(b) \ge f(c)$. But

$$\begin{aligned} f(a) + f(b) &\ge f(a+b) \quad &(\textit{subadditive}) \\ &\ge f(c) \quad &(\textit{nondecreasing}), \end{aligned}$$

as required. ■

Terpe [18] noticed that if $g:[0,\infty) \to [0,\infty)$ is non-increasing, then $\int_0^x g(t)\,dt$ is subadditive, and thus by Proposition 2.3, it is metric-preserving.

Another application of Proposition 2.3 involves concave functions: A function $f:[0,\infty) \to [0,\infty)$ is *concave* if for all $x, y \ge 0$,

$$f\left(\frac{x+y}{2}\right) \ge \frac{f(x)+f(y)}{2}.$$

Clearly, f is concave if and only if $-f$ is convex on $[0,c]$ for every $c > 0$. Ger and Kuczma [12] showed that concave amenable functions must be nondecreasing; since such functions are easily shown to be subadditive, we can use Proposition 2.3 again to conclude that they are also metric-preserving.

Exercise 2. Use either Proposition 2.3 or the fact that concave amenable functions are always metric-preserving to show that $\log_a(1+x)$, with $a > 1$, and x^r, with $0 < r \le 1$, are metric-preserving.

Another interesting example of a metric-preserving function was discovered by Doboš [7] who showed that the extended Cantor function (extended to have value 1 for all $x > 1$) is subadditive, and hence, by Proposition 2.3, is metric-preserving.

Our examples so far have been both nondecreasing and continuous. A simple example of a discontinuous nondecreasing metric-preserving function is

$$f(x) = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{otherwise}. \end{cases}$$

Proposition 2.3 ensures that this function is metric-preserving. It is also possible to obtain a continuous, metric-preserving function that fails to be nondecreasing. In order to construct this and other related examples, we need the notion of a *triangle triplet*, which is used to characterize metric-preserving functions. This notion first appeared in Sreenivasan's early paper **[16]**, though the terminology itself did not appear in the literature until **[2]**.

Definition 2.4. A *triangle triplet* is a triple (a, b, c) of nonnegative reals for which $a \le b + c, b \le a + c$, and $c \le a + b$; equivalently, $|a - b| \le c \le a + b$.

Triangle triplets are precisely those triples of nonnegative reals that are of the form $(d(x, y), d(y, z), d(x, z))$ for some metric space (X, d) and some $x, y, z \in X$. This observation follows from Proposition 2.5 and the proof of Proposition 2.6.

Proposition 2.5. *If (X, d) is a metric space and $x, y, z \in X$, then $(d(x, y), d(y, z), d(x, z))$ is a triangle triplet.*

Proof: This is immediate from the triangle inequality.

Proposition 2.6 [2]. *Suppose f is amenable. Then the following are equivalent:*

(1) *f is metric-preserving;*
(2) *for each triangle triplet $(a, b, c), (f(a), f(b), f(c))$ is a triangle triplet.*

Proof of (1) $\Rightarrow$ (2). Given a triangle triplet (a, b, c), let d be the usual metric on $\mathbf{R}^2$. A straightforward argument using elementary geometry shows that there are $u, v, w \in \mathbf{R}^2$ such that $d(u, v) = a, d(v, w) = b$, and $d(u, w) = c$. The result now follows from Proposition 2.5. ∎

Proof of (2) $\Rightarrow$ (1). Given (X, d), we verify that $f \circ d$ is a metric. Properties (M1) and (M2) are immediate. For (M3), use (2) and the fact that $(d(x, y), d(y, z), d(x, z))$ is always a triangle triplet for $x, y, z \in X$. ∎

For metric-preserving functions f, we obtain from Proposition 2.6(2) the inequality

$$|f(a) - f(b)| \le f(|a - b|) \tag{2.2}$$

by letting $c = |a - b|$.

Das **[5]** offers an alternative to Proposition 2.6(2) in his characterization of metric-preserving functions. A second alternative is the following:

Exercise 3(**[16]**, **[18]**). Show that Proposition 2.6(2) can be replaced by

$$\text{for each triangle triplet } (a, b, c),\ f(a) \le f(b) + f(c). \tag{2$'$}$$

The proof of Proposition 2.6 shows that an amenable function f is metric-preserving if and only if $f \circ d$ is a metric on $\mathbf{R}^2$ whenever d is. Doboš gives an interesting example that shows $\mathbf{R}^2$ cannot be replaced by $\mathbf{R}$ **[6]**. He builds a variation f of the extended Cantor function that preserves metrics on $\mathbf{R}$ and has the property that $\liminf_{x > 0} f(x) = 0$. The next proposition shows that such functions cannot be metric-preserving:

Proposition 2.7. *Suppose f is metric-preserving.*

(1) *For each $x_0 > 0$, there is an $\epsilon > 0$ such that $f(x) \geq \epsilon$ for each $x \geq x_0$. In particular,* $\liminf_{x>0} f(x) > 0$, *and $(x, 0)$ is not a limit point of the graph of f for any $x > 0$.*

(2) *If f is discontinuous at 0, there is some $\epsilon > 0$ such that $f(x) > \epsilon$ for all $x > 0$.*

Proof of (1). If the assertion is false, there are $x_0 > 0$ and a sequence $\langle x_n \rangle_n$ such that $x_n > x_0$ for all n, and $\langle f(x_n) \rangle_n \longrightarrow 0$. Let n be such that $f(x_n) < f(x_0)/2$. Then (x_n, x_n, x_0) is a triangle triplet, but $(f(x_n), f(x_n), f(x_0))$ is not. ■

Proof of (2). If (2) is false, it follows from (1) that there is a decreasing sequence $\langle x_n \rangle_n$ such that $\langle x_n \rangle_n \longrightarrow 0$ and $\langle f(x_n) \rangle_n \longrightarrow 0$. By discontinuity at 0, there are $\epsilon > 0$ and a sequence $\langle y_n \rangle_n$ converging to 0 such that $f(y_n) \geq \epsilon$ for all n. Now let n be such that $x_n < \epsilon/2$ and let m be such that $y_m < x_n$. Then (x_n, x_n, y_m) is a triangle triplet, but $(f(x_n), f(x_n), f(y_m))$ is not. ■

Proposition 2.7 shows that metric-preserving functions cannot have the x-axis as a horizontal asymptote; thus, the function $x/(1 + x^2)$ is not metric-preserving.

Using Proposition 2.6, we can now exhibit quite a variety of discontinuous metric-preserving functions. We call an amenable function f *tightly bounded* if there exists a $v > 0$ such that $f(x) \in [v, 2v]$ for all $x > 0$.

Proposition 2.8 [2]. *If f is amenable and tightly bounded, then f is metric-preserving.*

Proof: Let $v > 0$ be such that $f(x) \in [v, 2v]$ for all $x > 0$, and let (a, b, c) be a triangle triplet. Since the cases in which $abc = 0$ are trivial, we assume $abc > 0$. Then $f(a) \leq 2v = v + v \leq f(b) + f(c)$, and Exercise 3 gives the desired conclusion. ■

Any amenable, tightly bounded function is necessarily discontinuous at 0. It follows that there are $2^{\mathbf{c}}$ tightly bounded, amenable functions (where $\mathbf{c}$ is the cardinality of $\mathbf{R}$), so "most" metric-preserving functions are not continuous. A typical pathological example that one can construct with Proposition is the following:

Proposition 2.9. *There exists a metric-preserving function that is nowhere continuous and nowhere of bounded variation.*

Proof: Let $\{A, B\}$ be a partition of $(0, \infty)$ such that both A and B are dense in $(0, \infty)$. Define $f: [0, \infty) \to [0, \infty)$ by

$$f(x) = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x \in A \\ 2 & \text{if } x \in B. \end{cases}$$

Since f is amenable and tightly bounded, it is metric-preserving; because of the choice of A and B, f has the required pathologies. ■

The example given in Proposition 2.9 shows, in particular, that metric-preserving functions need not be nondecreasing. Pokorný **[15]** has isolated a fairly natural class of amenable functions for which all metric-preserving functions must be

nondecreasing: Define

$$\mathscr{G} = \{g : \text{for some periodic } h : [0,\infty) \to [0,\infty),\ g(x) = x + h(x) \text{ for all } x \geq 0\}.$$

An example of a member of $\mathscr{G}$ is $x + |\sin(x)|$. Pokorný showed that for amenable members f of the class $\mathscr{G}$, f is metric-preserving if and only if f is nondecreasing and subadditive.

Proposition 2.9 also shows that metric-preserving functions need not be of bounded variation on any interval. Nonetheless, most of our examples of metric-preserving functions have this property. Terpe **[17]** formulated a sufficient condition, involving the notion of *bounded gradient*: Given $r > 0$, we say that a metric-preserving function f is of *r-bounded gradient at* 0 if there is some $h > 0$ such that $f(x) \leq rx$ for all $x \in [0, h]$. And we say that f is *of bounded gradient at* 0 if there is some $r > 0$ such that f is of r-bounded gradient at 0.

Proposition 2.10 [17]. *If f is metric-preserving and of bounded gradient at* 0, *then f is of bounded variation on each closed interval lying in* $[0,\infty)$.

We postpone the proof of Proposition 2.10 until Section 4. There, we show that a metric-preserving function is of bounded gradient at 0 if and only if the derivative of f at 0 exists and is finite. We are establishing a global property of f (namely, bounded variation on each closed interval) based on the behavior of f at 0. This theme reappears when we consider continuity in the next section.

For the remainder of this section, we discuss techniques for building new metric-preserving functions from old and apply these to answer several natural questions:

- Q1. Can a metric-preserving function be strictly decreasing on an interval (a,∞), $a \geq 0$?
- Q2. Can a *continuous* metric-preserving function be strictly decreasing on an interval (a,∞), $a \geq 0$?
- Q3. Must every continuous, nondecreasing metric-preserving function be concave?
- Q4. Must every discontinuous metric-preserving function be tightly bounded?
- Q5. Must every metric-preserving function that is continuous at 0 be continuous?

To answer Question Q1, we first show that every bounded function $[0,\infty) \to [0,\infty)$ has an upward translation that is tightly bounded. For each $f : [0,\infty) \to [0,\infty)$ and each $r > 0$ we define

$$U_{f,r}(x) = \begin{cases} 0, & \text{if } x = 0 \\ f(x) + r, & \text{if } x > 0. \end{cases}$$

Proposition 2.11. *Suppose $f : [0,\infty) \to [0,\infty)$ is bounded above. Then there is an $r_0 > 0$ such that $U_{f,r}$ is metric-preserving for all $r \geq r_0$.*

Proof: Let r_0 be an upper bound for f and note that $U_{f,r}$ is tightly bounded for all $r \geq r_0$. ∎

Example 2.12. A *metric-preserving function* that is strictly decreasing on $(0, \infty)$. Define

$$g(x) = \begin{cases} 0 & \text{if } x = 0 \\ 1 + \dfrac{1}{x+1} & \text{if } x > 0. \end{cases}$$

Now, $g = U_{f,1}$ where

$$f(x) = \begin{cases} 0 & \text{if } x = 0 \\ \dfrac{1}{x+1} & \text{if } x > 0. \end{cases}$$

By Proposition 2.11, g is metric-preserving and is decreasing on $(0, \infty)$. This example answers Question Q1.

The next proposition provides a tool for answering Questions Q2 and Q3.

Proposition 2.13 [2, Proposition 2.16]. *Suppose f is metric-preserving and suppose $c, r > 0$. Define $T_{f,c,r} : [0, \infty) \to [0, \infty)$ by*

$$T_{f,c,r}(x) = \begin{cases} rx & \text{if } x \in [0, c) \\ f(x) & \text{otherwise.} \end{cases}$$

Then $T_{f,c,r}$ is metric-preserving if and only if $f(c) = rc$ and $|f(x) - f(y)| \leq r|x - y|$ for all $x, y \in [c, \infty)$. ■

In [**11**], the authors generalize this result, replacing the function rx in the defintion of $T_{f,c,r}$ by a concave metric-preserving function $g : [0, \infty) \to [0, \infty)$. Let $T_{f,g,c}$ denote the function defined from f and g in this way. As the authors of [**11**] show, if $|x - y| \leq c$ implies $|f(x) - f(y)| \leq g(|x - y|)$ for all $x, y \geq c$, then $T_{f,g,c}$ is metric-preserving.

Example 2.14. *A metric-preserving, continuous function that is strictly decreasing on* $(1, \infty)$. Let g be as in Example 2.12. Define

$$T(x) = \begin{cases} \frac{3}{2}x & \text{if } x \in [0, 1] \\ g(x) & \text{otherwise.} \end{cases}$$

Clearly, T is continuous and strictly decreasing on $(1, \infty)$. Since $T = T_{g,1,1}$, Proposition 2.13 ensures that T is metric-preserving. This example settles Question Q2. It also shows that continuous metric-preserving functions need not be nondecreasing.

Example 2.15 [18]. *A continuous, nondecreasing, metric-preserving function that is not concave.* Define

$$f(x) = \begin{cases} 1 & \text{if } 0 \leq x < 2 \\ x - 1 & \text{if } 2 \leq x < 3 \\ 2 & \text{otherwise.} \end{cases}$$

Since f is tightly bounded, f is metric-preserving. Define

$$T(x) = \begin{cases} x & \text{if } x \in [0, 1] \\ f(x) & \text{otherwise.} \end{cases}$$

Clearly T is continuous and nondecreasing; T is not concave since

$$T\left(\frac{a+b}{2}\right) < \frac{T(a)+T(b)}{2}$$

when $a = 1$ and $b = 3$. Since $T = T_{f,1,1}$, Proposition 2.13 can be applied to show T is metric-preserving. This example settles Question Q3.

Exercise 4 [13]. Use Propositions 2.11 and Proposition 2.13 to show that Jůza's function (1.1) is metric-preserving.

To answer Question Q4, we invoke one of the closure properties of the class of metric-preserving functions. We summarize these in the following theorem; we omit the straightforward proofs.

Theorem 2.16 [1], [2], [17].

(1) *If* f, g *are metric-preserving and* $m > 0$, *then each of* $f \circ g, f + g, mf$ *and* $\max(f, g)$ *is metric-preserving.*
(2) *If* $\langle h_n \rangle_n$ *are metric-preserving functions that converge pointwise to a function* h *and* $h(x) > 0$ *for all* x, *then* h *is metric-preserving. Likewise, if* $\Sigma_{n=1}^{\infty} h_n$ *converges to a function* $\overline{h}$, *where each function* h_n *is metric-preserving, then* $\overline{h}$ *is metric-preserving.*
(3) *If* S *is any set of metric preserving functions that is pointwise bounded and if we define* $g(x) = \sup\{f(x) : f \in S\}$, *then* g *is metric-preserving.*

Example 5 [2]. *A discontinuous and metric-preserving function that is not tightly bounded.* Define

$$f(x) = \begin{cases} 0 & \text{if } x = 0 \\ 1 + |x - 1| & \text{otherwise.} \end{cases}$$

The function f is discontinuous at 0 and not tightly bounded. Now, $f = \max(g, h)$, where $g(x) = x$ and

$$h(x) = \begin{cases} 0 & \text{if } x = 0 \\ 1 + |x - 1| & \text{if } x \in (0, 2) \\ 2 & \text{otherwise.} \end{cases}$$

Since h is metric-preserving (because it is tightly bounded), and g is metric-preserving, it follows from Theorem 2.16(1) that f is metric-preserving as well. This example settles Question Q4.

We postpone a discussion of Question Q5 until the next section, where it is a central topic.

3. STRONGLY METRIC-PRESERVING FUNCTIONS. In this section we characterize the metric-preserving functions that are strongly metric-preserving. An important theme here is the significance of the behavior of a metric-preserving function at 0: We show that such an f is strongly metric-preserving if and only if it is continuous at 0.

We begin with some notation and an observation. For a metric space (X, d), $x \in X$, $\epsilon > 0$, write:

$$N(d, x, \epsilon) = \{y \in X : d(x, y) < \epsilon\}.$$

Lemma 3.1. *Suppose f is metric-preserving. Then the following are equivalent*:

(1) *f is discontinuous at* 0;
(2) *$f \circ d$ is a discrete metric for every metric d.*

Proof of (1) $\Rightarrow$ (2). Let (X, d) be a metric space. By Proposition 2.7, there is an $\epsilon > 0$ such that $f(z) > \epsilon$ for all $z > 0$. Then $N(f \circ d, x, \epsilon) = \{x\}$ for each $x \in X$, as required. ■

Proof of (2) $\Rightarrow$ (1). Let d be the usual metric on $\mathbf{R}$ and let $\epsilon > 0$ be such that $N(f \circ d, 0, \epsilon) = \{0\}$. It follows that there is a sequence $\langle x_n \rangle_n$ of positive numbers converging to 0 (relative to d) such that $\epsilon < f(d(x_n, 0)) = f(x_n)$ for all n. This establishes (1). ■

The next theorem first appeared in [**2**]; one direction of the theorem was observed in [**16**].

Theorem 3.2 [2]. *A metric-preserving function is strongly metric-preserving if and only if it is continuous at* 0.

Proof: One direction follows from Lemma 3.1. For the other direction, suppose f is continuous at 0 and metric-preserving. Let (X, d) be a metric space. We show that $f \circ d$ and d are equivalent metrics. Let $\epsilon > 0$ and $x \in X$. By continuity, let $\delta \leq \epsilon$ be such that $f(z) < \epsilon$ whenever $0 \leq z < \delta$. Then $N(d, x, \delta) \subseteq N(f \circ d, x, \epsilon)$. Hence, the d-topology refines the $f \circ d$-topology. To show the converse, again start with $x \in X$ and let $r > 0$. Use Proposition 2.7(1) to obtain an $\epsilon > 0$ such that $f(z) \geq \epsilon$ for all $z \geq r$. But now $N(f \circ d, x, \epsilon) \subseteq N(d, x, r)$, and we are done. ■

In [**2**], the authors develop Theorem 3.2 further by providing necessary and sufficient conditions on a metric-preserving function f for d and $f \circ d$ to be *uniformly* equivalent as well.

As we now show, continuity at 0 forces a metric-preserving function to be continuous everywhere; this result answers Question Q5 from Section 2.

Theorem 3.3 [2]. *Suppose f is metric-preserving and continuous at* 0. *Then f is continuous on* $[0, \infty)$.

Proof: Assume that f is not continuous at some $x_0 > 0$. Let $\epsilon > 0$ be such that there are z arbitrarily close to x_0 for which $|f(z) - f(x_0)| \geq \epsilon$. By continuity at 0, let $\delta < x_0/2$ be such that $0 \leq a < \delta$ implies $f(a) < \epsilon$. Now pick z_0 so that $|z_0 - x_0| < \delta$ and $|f(z_0) - f(x_0)| \geq \epsilon$. Let $a_0 = |z_0 - x_0|$.

Case 1. $f(z_0) \geq f(x_0) + \epsilon$.

If $x_0 + a_0 = z_0$, then $f(x_0) + f(a_0) < f(x_0) + \epsilon \leq f(x_0 + a_0)$, which violates subadditivity.

On the other hand, if $z_0 + a_0 = x_0$, notice that (x_0, z_0, a_0) is a triangle triplet, and in particular that $x_0 - z_0 = a_0 < \delta$. But since $f(z_0) - f(x_0) \geq \epsilon$ and $f(a_0) < \epsilon$, $(f(x_0), f(z_0), f(a_0))$ is not a triangle triplet, which violates Proposition 2.3.

Case 2. $f(x_0) \geq f(z_0) + \epsilon$.

The proof in this case is similar to that in Case 1, and we omit it.

In each case, we have obtained a contradiction from the assumption that x_0 is a point of discontinuity, as required. ■

Thus, for a metric-preserving function f, the global properties of continuity and being strongly metric-preserving are completely determined by the behavior of f at 0. And continuity of f at 0 is determined by a property that is apparently even weaker: It follows from Proposition 2.7(2) that f is continuous at 0 if and only if, for each $\epsilon > 0$, there is an $x > 0$ with $f(x) < \epsilon$. We have proved the following:

Theorem 3.4 [2]. *Suppose f is metric-preserving. Then the following are equivalent:*

(1) *f is strongly metric-preserving;*
(2) *f is continuous at* 0;
(3) *f is continuous on* $[0, \infty)$;
(4) *for each $\epsilon > 0$, there is an $x > 0$ with $f(x) < \epsilon$.* ■

As an application of Theorem 3.4, we give a proof of a result in [1] that improves upon Corollary 2.2(A):

Theorem 3.5. *If f is metric-preserving and is convex on $[0, c]$ for some $c > 0$, then f is linear on* $[0, c]$.

Proof: Let f be metric-preserving and convex on [0, c]. We establish the conclusion of the theorem from the following three claims:

Claim 1. *For each $x \in [0, c]$ and each positive integer n, $f(x/2^n) = f(x)/2^n$.*

Claim 2. *The function f is continuous.*

Claim 3. *Whenever $0 < x \leq y \leq c$, $f(x)/x \leq f(y)/y$.*

Using these claims, we prove the result by showing that $f(x) = (f(c)/c)x$ for all $x \in [0, c]$. Since this relation is obvious for $x = 0$, let $x \in (0, c]$, and let n be such that $c/2^n \leq x$. Then by Claims 1 and 3,

$$\frac{f(c)}{c} = \frac{f\left(\frac{c}{2^n}\right)}{\frac{c}{2^n}} \leq \frac{f(x)}{x} \leq \frac{f(c)}{c},$$

as required.

We turn to the proofs of the claims. Claim 1 is proved by combining parts (1) and (2) of Exercise 1. For Claim 2, we use Claim 1 and Theorem 3.4(4): For any $\epsilon > 0$, we obtain x for which $f(x) < \epsilon$ by setting $x = \epsilon/2^n$, where n is such that $f(\epsilon)/2^n < \epsilon$.

To prove Claim 3, let $A = \{u \in [0, c] : f(x)/x \leq f(y)/y$ whenever $0 < x \leq y \leq u\}$. Vacuously, A is nonempty. Let $z = \sup A$; we prove $A = [0, c]$ by showing $z = c$. Seeking a contradiction, assume $z < c$. There are two cases to consider:

Case 1. $z \notin A$. From our assumptions, it follows that there is an $x_0 < z$ such that $f(x)/x > f(z)/z$ whenever $x_0 \leq x < z$. For each such x, let $g_x : [0, \infty) \to [0, \infty)$

denote the function whose graph is the line through $(0,0)$ and $(x, f(x))$. By the choice of z, whenever $x_0 \leq x \leq y \leq z$, we have $g_{x_0}(z) > f(z)$ and $g_x(y) \geq g_{x_0}(y)$. By continuity of g_{x_0}, there is a δ such that $0 < \delta \leq z - x_0$ and $g_{x_0}(x) > f(z)$ whenever $0 < z - x \leq \delta$. Let $x_1 = z - \delta$, and let $\epsilon = g_{x_0}(x_1) - f(z)$. Then, whenever $0 < z - x \leq \delta$,

$$|f(x) - f(z)| = g_x(x) - f(z) \geq g_{x_0}(x) - f(z) \geq g_{x_0}(x_1) - f(z) = \epsilon,$$

which contradicts the continuity of f at z.

Case 2. $z \in A$. By our assumptions, we can find y such that $f(z)/z > f(y)/y$ where $y > z$ and y is arbitrarily close to z. Pick such a y with $y - z < z$. Set $x = 2z - y$. Then $z = (x + y)/2$, and by a straightforward computation,

$$\frac{f(z) - f(x)}{z - x} \leq \frac{f(y) - f(z)}{y - z}. \tag{3.1}$$

However, it is easy to verify that

$$\frac{f(x)}{x} \leq \frac{f(z)}{z} \text{ implies } \frac{f(z)}{z} \leq \frac{f(z) - f(x)}{z - x}, \tag{3.2}$$

and

$$\frac{f(y)}{y} < \frac{f(z)}{z} \text{ implies } \frac{f(y) - f(z)}{y - z} < \frac{f(z)}{z}. \tag{3.3}$$

Combining the conclusions of (3.2) and (3.3), we have

$$\frac{f(z) - f(x)}{z - x} > \frac{f(y) - f(z)}{y - z},$$

which contradicts (3.1). This completes the proof of Claim 3 and the theorem. ∎

Metric-preserving functions can be viewed as a tool for producing new metrics of the form $f \circ d$ on a given metric space (X, d). The results of this section show that the usefulness of this tool does not lie in generating topologically distinct metrics; indeed, at most two distinct metrics, up to topological equivalence, can be obtained in this way: the discrete metric and d itself. More useful is the fact that whenever X has cardinality at least 2, there are $\mathbf{c}$ distinct metrics on X of the form $f \circ d$, where f is metric-preserving. This fact suggests that the class of metric-preserving functions may be a rich source for constructing metrics that are topologically equivalent to d but that exhibit new, mathematically interesting properties. Indeed, Jůza's function (1.1) is just this kind of example.

4. METRIC-PRESERVING FUNCTIONS AND DIFFERENTIABILITY. Mirroring the situation for continuity, the notion of differentiability partitions the class of metric-preserving functions into two rather different subclasses determined by the value of the derivative of each function at 0. We shall see that the (extended) derivative of such a function always exists at 0; the central question is whether the derivative is finite or infinite. Functions with finite derivative form a well-behaved class of continuous functions that are differentiable almost everywhere; functions with infinite derivative, by contrast, can be very unruly—they can be continuous, nowhere differentiable (in the finite sense), and even, as we saw in Section 2, nowhere continuous. In this section we outline proofs of these results, which we have extracted from [**1**].

We first show that for any metric-preserving function f, $f'(0)$ exists in the extended sense. The proof naturally divides into two parts depending on whether the set $K_f = \{r > 0 : f(x) \le rx \text{ for all } x \ge 0\}$ is empty. In the course of the proof, we show that $f'(0) < +\infty$ if and only if $K_f \ne \varnothing$, and $f'(0) = +\infty$ if and only if $K_f = \varnothing$. The next lemma is the first step in proving the result for the latter case.

Lemma 4.1 [1]. *If f is metric-preserving and $0 < x \le y$, then $f(y)/y \le 2f(x)/x$.*

Proof: Let n be a positive integer such that

$$2^{n-1} \le \frac{y}{x} < 2^n. \tag{4.1}$$

Then $(x, x, y/2^{n-1})$ is a triangle triplet since $y/2^{n-1} < 2x$. Thus, $f(y)/2^{n-1} \le f(y/2^{n-1}) \le 2f(x)$, where the first inequality follows from Exercise 1(1). Hence, using (4.1), $f(y) \le 2^{n-1}(2f(x)) \le 2yf(x)/x$, and the result follows. ∎

We can now prove that $f'(0)$ exists and is infinite when $K_f = \varnothing$: Let n be a positive integer. Since $K_f = \varnothing$, we can pick $y > 0$ such that $f(y) \ge 2ny$. Let $x \in (0, y]$. By Lemma 4.1, $2n \le f(y)/y \le 2f(x)/x$. But now we have shown that for each integer $n > 0$, there is $y > 0$ such that $f(x)/x \ge n$ whenever $0 < x \le y$, as required.

We turn to the case in which $K_f \ne \varnothing$. Suppose f is metric-preserving and that there is an $h > 0$ such that $f(x) \le rx$ for all $x \in [0, h]$ (that is, f is of r-bounded gradient at 0, as in Proposition 2.10). We show that in fact, $f(x) \le rx$ for all $x \ge 0$. To see this, let $x \ge 0$ and let n be a large enough integer so that $x/2n \le h$. By Exercise 1(1), $f(x)/2^n \le f(x/2^n) \le rx/2^n$, whence, $f(x) \le rx$. Combining this result with (2.2), we also have $|f(x) - f(y)| \le r|x - y|$ for all $x, y \ge 0$. Thus:

Proposition 4.2 [1]. *Suppose $r > 0$ and f is metric-preserving and of r-bounded gradient at 0. Then,*

(1) *$f(x) \le rx$ for all $x \ge 0$;*
(2) *$|f(x) - f(y)| \le r|x - y|$ for all $x, y \ge 0$.*G

The next result that we need is a generalization of Theorem 3.5:

Lemma 4.3 [1]. *Suppose f is metric-preserving and $r > 0$. If in every neighborhood of 0 there is a point a such that $f(a) = ra$, then there is an $h > 0$ such that $f(x) = rx$ for all $x \in [0, h]$.*

Proof: The hypothesis and Theorem 3.4(4) imply that f is continuous. Let $h > 0$ be such that $f(h) = rh$. Assume there is $x \in (0, h)$ with $f(x) \ne x$. Let $A = \{y \in [0, \infty) : f(y) = ry\}$. By continuity of f, $A \cap [0, x]$ is compact and so has a maximum element, which we denote by $m_{0,x}$; likewise, $A \cap [x, h]$ is compact, and we denote its minimum element by $m_{x,h}$.

If $f(x) > rx$, we show there is a number $u \in (m_{0,x}, x)$ such that $f(u) \le ru$, from which it follows, by continuity, that $f(z) = rz$ for some $z \in [u, x)$, contradicting the choice of $m_{0,x}$. To obtain u, let $y \in A$ with $0 < y < x - m_{0,x}$. Now let $u = y + m_{0,x}$ and observe that

$$f(y + m_{0,x}) \le f(y) + f(m_{0,x}) = ry + rm_{0,x} = r(y + m_{0,x}).$$

Similarly, if $f(x) < rx$, one obtains a $u \in (x, m_{x,h})$ such that $f(u) \geq ru$, yielding a contradiction, as before. Here, pick $z \in A$ with $0 < z < m_{x,h} - x$ and set $u = m_{x,h} - z$. We leave to the reader the verification that u has the required property. ■

Now we prove that $f'(0)$ exists and is finite in the case $K_f \neq \varnothing$. By Theorem 3.4, f is continuous, whence K_f is closed. Let $r_0 = \min K_f$. We show

$$r_0 = \lim_{x \to 0} \frac{f(x)}{x}. \tag{4.2}$$

Let $\epsilon > 0$. We claim that:

$$\text{for each } h > 0, \text{ there is an } x \in (0, h] \text{ such that } f(x) > (r_0 - \epsilon)x. \tag{4.3}$$

To see this, assume instead that there is an $h > 0$ such that for all $x \in [0, h]$, $f(x) \leq r_1 x$, where $r_1 = r_0 - \epsilon$. Thus, f is of r_1-bounded gradient at 0, and so by Proposition 4.2(1), $f(x) \leq r_1 x$ for all $x \geq 0$, which contradicts the choice of r_0.

Next, we show that

$$\text{there exists an } h > 0 \text{ such that } f(x) > (r_0 - \epsilon)x \text{ for all } x \in (0, h]. \tag{4.4}$$

Assume instead that

$$\text{for each } h > 0, \text{ there exists an } x \in [0, h] \text{ such that } f(x) \leq (r_0 - \epsilon)x. \tag{4.5}$$

Let $h > 0$. By (4.3), there is an $x_1 \in (0, h]$ such that $f(x_1) > (r_0 - \epsilon)x_1$, and by (4.5), there is an $x_2 \in (0, h]$ such that $f(x_2) \leq (r_0 - \epsilon)x_2$. By the continuity of f, there is an $x_3 \in (0, h]$ such that $f(x_3) = (r_0 - \epsilon)x_3$. By Lemma 4.3, $f(x) = (r_0 - \epsilon)x$ holds on some neighborhood of 0, contradicting (4.3). This proves (4.4).

Now since $r_0 \in K_f$, we also have $f(x) < (r_0 + \epsilon)x$ for each $x > 0$. Thus, combining these results, we obtain: for each $\epsilon > 0$, there exists an $h > 0$ such that $r_0 - \epsilon < f(x)/x < r_0 + \epsilon$ whenever $0 < x \leq h$; that is, (4.2) holds, as required.

We have proved:

Theorem 4.4 [1]. *Let f be a metric-preserving function. Then $f'(0)$ exists (in the extended sense).* ■

We now show that a metric-preserving function f with finite derivative at 0 must be differentiable almost everywhere. We begin with a key lemma:

Lemma 4.5 [1]. *Suppose f is metric-preserving and $f'(0) < +\infty$. Then*

(1) $f(x) \leq f'(0)$ *for all* $x \geq 0$;
(2) $|f(x) - f(y)| \leq f'(0)|x - y|$ *for all* $x, y \geq 0$.

Proof: To prove (1), let $\epsilon > 0$. Since $f'(0) < +\infty$, there is an $h > 0$ such that

$$f(x) \leq (f'(0) + \epsilon)x \tag{4.6}$$

for all $x \in [0, h]$; that is, f is of $(f'(0) + \epsilon)$-bounded gradient at 0. By Proposition 4.2, (4.6) holds for all $x \geq 0$. Since $\epsilon > 0$ was arbitrary, the result follows. Part (2) can be proved by again applying (2.2). ■

The proof of Lemma 4.5(1) shows that if f is metric-preserving and $f'(0) < +\infty$, then f is of bounded gradient at 0. The converse is also true, and follows immediately from Theorem 4.4. Thus:

Corollary 4.6. *Let f be a metric-preserving function. Then $f'(0) < +\infty$ if and only if f is of bounded gradient at* 0. ∎

Our target theorem falls out directly from Lemma 4.5(2) and establishes Proposition 2.10:

Theorem 4.7 [1]. *Suppose f is metric-preserving and $f'(0) < +\infty$. Then f is of bounded variation on each closed interval lying in $[0, \infty)$. Hence, f is differentiable almost everywhere.* ∎

Finally, we consider the subclass of metric-preserving functions f for which $f'(0) = +\infty$. The following example, due to Doboš and Piotrowski, is a slight modification of Van der Waerden's continuous nowhere differentiable function [3].

Example 4.8 [11]. *A metric-preserving function that is continuous and nowhere differentiable.* Define $h : [0, \infty) \to [0, \infty)$ by

$$h(x) = \begin{cases} x & \text{if } x \leq \frac{1}{2} \\ \frac{1}{2} + \left|x - [x] - \frac{1}{2}\right| & \text{if } x > \frac{1}{2}, \end{cases}$$

where $[a]$ denotes the integer part of a. It is easy to verify that $h = T_{g, \frac{1}{2}1}$ for some tightly bounded function g (recall Proposition 2.13), and so h is metric-preserving. Likewise, for each integer $n \geq 0$, $h(2^n \cdot x)$ is metric-preserving, and using Theorem 4.9(1), so is $h(2^n \cdot x)/2^n$. Theorem 4.10(2) ensures that

$$f(x) = \sum_{n=0}^{\infty} \frac{h(2^n \cdot x)}{2^n}$$

is metric-preserving as well. The proof that f is continuous and nowhere differentiable is essentially the same as Van der Waerden's.

The extent to which the class of metric-preserving functions is structured around their behavior at 0 has been a striking theme in this brief survey. Whether a metric-preserving function f transforms each metric d to a discrete metric or to a metric that is topologically equivalent to d is determined by whether f is continuous at 0. And whether f has the property of being (finitely) differentiable almost everywhere but nowhere infinitely differentiable is determined by whether $f'(0)$ is finite or infinite. Although the results presented here offer many possible directions for generalization and further study, one of the most compelling is this:

> *Which behaviors of a metric-preserving function f at 0—such as continuity at 0 or "$f'(0) < +\infty$"—determine interesting global properties of f?*

REFERENCES

1. J. Borsík and J. Doboš, On metric preserving functions, *Real Anal. Exchange* 13 (1987–88) 285–293.
2. ______, Functions whose composition with every metric is a metric, *Math. Slovaca* 31 (1981) 3–12 (in Russian).
3. P. Billingsley, Van der Waerden's continuous nowhere differentiable function, *Amer. Math. Monthly* 89 (1982) 691.
4. A. Bruckner, Differentiation of Real Functions, Lecture Notes In Mathematics 659, Springer-Verlag, New York, 1978.
5. P. P. Das, Metricity preserving transforms, *Pattern Recognition Letters* 10 (1989) 73–76.

6. J. Doboš, On modifications of the Euclidean metric on reals, *Tatra Mt. Math. Publ.* 8 (1996) 51–54.
7. ______, The standard Cantor function is subadditive, *Proc. Amer. Math. Soc.* 124 (1996) 3425–6.
8. ______, A survey of metric-preserving functions, *Questions Answers Gen. Topology* 13 (1995) 129–133.
9. J. Doboš, Z. Piotrowski, When distance means money, *Internat. J. Math. Ed. Sci. Tech.* 28 (1997) 513–518.
10. ______, A note on metric-preserving functions, *Internat. J. Math. Math. Sci.* 19 (1996) 199–200.
11. ______, Some remarks on metric-preserving functions, *Real Anal. Exchange* 19 (1993–94) 317–320.
12. R. Ger and M. Kuczma, On the boundedness and continuity of convex functions and additive functions, *Aequationes Math.* 4 (1970) 157–162.
13. M. Jůza, A note on complete metric spaces, *Matematicko-fyzikálny časopis SAV* 6 (1956) 143–148 (in Czech).
14. J. Kelley, *General Topology*, Springer-Verlag, New York, 1955.
15. I. Pokorný, Some remarks on metric preserving functions, *Tatra Mt. Math. Publ.* 2 (1993) 65–68.
16. T. K. Sreenivasan, Some properties of distance functions, *J. Indian Math. Soc.* (*N.S.*) 11 (1947) 38–43.
17. F. Terpe, Some properties of metric preserving functions, *Proc. Conf. Topology, Measure and Fractals*, Math. Res. 66, Akademie-Verlag, Berlin, 1992, pp. 214–217.
18. ______, Metric preserving functions, *Proc. Conf. Topology and Measure IV*, Greifswald, 1984, pp. 189–197.
19. W. A. Wilson, On certain types of continuous transformations of metric spaces, *Amer. J. Math.* 57 (1935) 62–68.

PAUL CORAZZA received his Ph.D. from Auburn University with a specialization in set theory. He has worked at the University of Wisconsin and at Maharishi International University as an assistant professor of mathematics. He is now a software engineer at Telegroup, a telecommunications company. His research interests include the theory of large cardinals, applications of set theory to real analysis, applications of category theory to computer science, and connections between the philosophy and mathematics of the infinite.
Maharishi University of Management, c/o 310 E. Washington Ave., Fairfield, IA 52556
pcorazza@kdsi.net

Someone wrote a book called *The Joy of Math.*
Maybe I'll write a book called the *The Pathos of Math.*
For through the night I wander
between intuition and calculation
between examples and counter-examples
between the problem itself and what it has led to.
I find special cases with no determining vertices.
I find special cases with only determining vertices.
I weave in and out.
I rock to and fro.
I am the wanderer
with a lemma in every port.

Contributed by Marion Cohen, Drexel University, Philadelphia, PA

Magic Dice

Bernard D. Flury, Robert Irving, and M. N. Goria

1. INTRODUCTION. A magician offers her audience a betting game with two dice. With X and Y denoting the numbers shown by the first and the second die, respectively, the magician wins one ruble for 12 of the 36 possible outcomes (x, y), and loses 1 ruble for another set of 12 outcomes, as indicated in Table 1. No payment is made in the remaining cases. This seems to be a fair game, but in fact the two dice are not independent, as seen from their joint distribution displayed in Table 1. Soon enough the audience realizes that every time a ruble is paid it is in

TABLE 1. Joint Probabilities for six-sided magic dice.
Columns correspond to values of X; rows to values of Y. Entries are probabilities in multiples of $1/36$. The audience wins if $(X, Y) = (1,3), (1,5), (2,3), (2,5), (3,3), (3,6), (4,1), (4,4), (5,2), (5,4), (6,2)$, or $(6,4)$. The magician wins for 12 other (arbitrarily chosen) outcomes.

	1	2	3	4	5	6
6	1	2	0	1	1	1
5	0	0	2	1	2	1
4	3	1	2	0	0	0
3	0	0	0	2	1	3
2	1	2	1	2	0	0
1	1	1	1	0	2	1

the magician's favor. This happens despite the fact that two observers who tally the frequencies of X and Y, respectively, find that both dice show each side with exactly the required relative frequency of $1/6$.

Now as almost everybody knows, marginal probabilities do not determine joint probabilities, and therefore the audience asks for a third observer. The magician agrees and lets someone tally the frequencies with which $X + Y$ takes values 2, $3, \ldots, 12$. Sure enough, these are found to be $1/36$, $2/36$, etc, just as expected if X and Y were independent fair dice. Hence a fourth observer is admitted who tallies $X - Y$, and finally a fifth observer who tallies $X + 2Y$. When asked to admit a sixth observer, however, the magician stops the game.

As can be verified from Table 1, none of the five observers studying the distributions of X, Y, $X + Y$, $X - Y$, and $X + 2Y$ is able to detect that something is wrong with the pair of dice. Indeed, all five observers find exactly what they expect if X and Y are independent regular dice, and the deviations of the joint probabilities from their fair value $1/36$ remains undetected.

The obvious question is, how many different observers can the magician admit without giving away the secret? To make this question clear, we formulate the rules of the game more precisely. Each time the magician is asked to admit another observer, she chooses a linear combination $aX + bY$ (with real coefficients a and b) that is not proportional to any of the previously assigned linear combinations. She constructs her dice such that she can admit as many observers as possible, yet be able to offer unfair bets. The maximum number of observers

that can be admitted is called the *magic number*. We investigate magic numbers for k–sided dice, $k \geq 2$. For six–sided dice the magic number is 5, and Table 1 gives a particular example where five observers can be admitted. It is straightforward (but tedious) to verify in Table 1 that any further linear combination would indeed reveal that some joint probabilities are not $1/36$. Showing that it is impossible to construct an unfair pair of dice that would admit more than five observers is somewhat more laborious; Theorem 6 gives us a final answer.

2. DEFINITION OF MAGIC NUMBERS. For a fixed integer $k \geq 2$, let (X, Y) denote a bivariate random variable taking values in the set $\{1, 2, \dots, k\} \times \{1, 2, \dots, k\}$ with probabilities p_{ij}.

Definition 1. A linear combination $Z = aX + bY$ is *proper* if its distribution is unchanged by setting all $p_{ij} = 1/k^2$.

For any linear combination $Z = aX + bY$ we have

$$\Pr[Z = m] = \sum_{(i,j) \in \mathscr{I}_m(a,b)} p_{ij},$$

where

$$\mathscr{I}_m(a, b) = \{(i, j) \in \mathbb{N}^2 : 1 \leq i \leq k, 1 \leq j \leq k, ai + bj = m\}.$$

Hence $Z = aX + bY$ is proper exactly if, for all integers m,

$$k^2 \cdot \Pr[Z = m] = \#(\mathscr{I}_m(a, b)),$$

where $\#(\mathscr{I})$ is the number of elements in the set $\mathscr{I}$.

Two linear combinations Z_1 and Z_2 are considered identical if $Z_1 = cZ_2$ for some $c \in \mathbb{R}$. The trivial linear combination $0 \cdot X + 0 \cdot Y$ is always excluded.

Definition 2. For $k \in \mathbb{N}$, $k \geq 2$, let $m(k)$ denote the maximum number of different linear combinations such that the following condition holds: It is possible to find joint probabilities p_{ij}, where not all p_{ij} are equal to $1/k^2$, such that all $m(k)$ linear combinations are proper. The number $m(k)$ is called the *magic number* for k–sided dice.

For $k \leq 4$, $m(k)$ can be found by hand, but for larger k a more systematic approach is needed.

3. COMPUTATION OF MAGIC DICE, AND PRELIMINARY RESULTS. For $k \geq 2$ there are only finitely many linear combinations that map the points $(i, j) \in \{1, \dots, k\} \times \{1, \dots, k\}$ into fewer than k^2 different points on the real line (which, in turn, would determine all p_{ij}). For instance, for $k = 3$ the only linear combinations to be considered are X, Y, $X + Y$, $X - Y$, $X + 2Y$, $X - 2Y$, $2X + Y$, and $2X - Y$. Only linear combinations with integer coefficients need to be considered, and a linear combination $Z = aX + bY$ can therefore be represented as a pair of integers (a, b). For each $k \geq 2$ the set of linear combinations to be considered is as follows.

Definition 3. The set of feasible linear combinations, or *feasible set*, for k–sided dice is the set $\mathscr{F}_k$ of pairs of integers (a, b) such that

(i) $0 \leq a \leq k - 1$, $-(k - 1) \leq b \leq k - 1$.
(ii) $ab = 0$ implies $a = 1$ or $b = 1$.
(iii) If both a and b are nonzero, then a and b are relatively prime.

Consider the matrix $\mathbf{U} = [u_{ij}]$, where $u_{ij} = k^2 p_{ij}$. For a given $(a, b) \in \mathscr{F}_k$, the linear combination $aX + bY$ generates a number $N_k(a, b)$ of linear equations in the variables u_{ij}. For example, for $k = 3$ and $(a, b) = (1, 1)$, the five equations

$$\begin{aligned} u_{11} &= 1 \\ u_{12} + u_{21} &= 2 \\ u_{13} + u_{22} + u_{31} &= 3 \\ u_{23} + u_{32} &= 2 \\ u_{33} &= 1 \end{aligned}$$

are generated. In the $N_k(a, b)$ equations generated by $(a, b) \in \mathscr{F}_k$ each of the variables u_{ij} occurs exactly once, and the right-hand side of each equation is the number of variables on the left hand side. Using the vec-operator that stacks the columns of a matrix on top of each other, and writing $\mathbf{1}_n$ for the n-vector with 1 in each position, the equations generated by $(a, b) \in \mathscr{F}_k$ can be written as

$$\mathbf{C}(a, b)\mathrm{vec}(\mathbf{U}') = \mathbf{C}(a, b)\mathbf{1}_{k^2}.$$

For $k = 3$ and $(a, b) = (1, 1)$, we obtain

$$\mathbf{C}(1,1) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

The matrix $\mathbf{C}(a, b)$ is binary, of dimension $N_k(a, b) \times k^2$, and has full row rank. For a subset $\mathscr{S} = \{(a_1, b_1), \ldots, (a_p, b_p)\} \subset \mathscr{F}_k$, let

$$\mathbf{C}_{\mathscr{S}} = \begin{bmatrix} \mathbf{C}(a_1, b_1) \\ \vdots \\ \mathbf{C}(a_p, b_p) \end{bmatrix}.$$

We refer to

$$\mathbf{C}_{\mathscr{S}}\mathrm{vec}(\mathbf{U}') = \mathbf{C}_{\mathscr{S}}\mathbf{1}_{k^2} \tag{1}$$

as the *system of equations generated by* $\mathscr{S}$. Defining $\mathbf{V} = \mathbf{U} - \mathbf{1}_k\mathbf{1}'_k$, we can write (1) as

$$\mathbf{C}_{\mathscr{S}}\mathrm{vec}(\mathbf{V}') = \mathbf{0}. \tag{2}$$

For a given subset $\mathscr{S} \subset \mathscr{F}_k$ we have to solve (2). If $\mathrm{rank}(\mathbf{C}_{\mathscr{S}}) = k^2$, then $\mathrm{vec}(\mathbf{V}') = \mathbf{0}$ is the only solution, so $\mathbf{U} = \mathbf{1}_k\mathbf{1}'_k$, and $p_{ij} = 1/k^2$ for all (i, j). If $\mathrm{rank}(\mathbf{C}_{\mathscr{S}}) < k^2$, then multiple solutions exist, and since $\mathrm{vec}(\mathbf{V}') = \mathbf{0}$ is always a solution, we can then obtain another solution for which the p_{ij} are probabilities. The magic number $m(k)$ is the largest cardinality of all subsets $\mathscr{S} \subset \mathscr{F}_k$ such that $\mathrm{rank}(\mathbf{C}_{\mathscr{S}}) < k^2$.

In preliminary calculations for k up to 24, Gaussian elimination was used to determine the rank of of $\mathbf{C}_{\mathscr{S}}$ exactly. In all cases considered, whenever $\mathscr{S}$ was a maximum cardinality subset it was possible to generate integer-valued solutions for $\mathbf{U}$, as in Table 1. (This is always possible, as we will see at the end of Section 5). The computational problem was huge for the larger values of k, and it was necessary to program the Gaussian elimination algorithm in integer arithmetic to retain full precision. Results obtained in this way are summarized in Table 2. Note that the choice of a new linear combination to be included is not always unique. For example, when going from $k = 5$ to $k = 6$, we have a choice of including one

TABLE 2. Magic Numbers and Related Quantities for k-sided dice, $2 \le k \le 24$.

$\mathscr{S}$ = largest subset of $\mathscr{F}_k$ such that rank$[\mathbf{C}_{\mathscr{S}}] < k^2$; $\mathbf{C}_{\mathscr{S}}$ = coefficient matrix generated by $\mathscr{S}$; $m(k)$ = magic number for k-sided dice. In the column labelled $\mathscr{S}$, each row shows only the linear combination introduced in addition to the ones already present in the preceding rows. *Note*: Magic dice for $k = 23$ and $k = 24$ can also be constructed using the linear combinations $(1,4)$ and $(4,1)$ instead of $(2,3)$ and $(3,2)$.

k	$\mathscr{S}$	rows($\mathbf{C}_{\mathscr{S}}$)	rank($\mathbf{C}_{\mathscr{S}}$)	$m(k)$
2	(1, 0) (0, 1)	4	3	2
3	(1, 1)	11	8	3
4	(1, −1)	22	15	4
5		28	21	4
6	(1, 2)	50	34	5
7	(2, 1)	78	48	6
8		90	60	6
9	(1, −2)	127	79	7
10	(2, −1)	170	99	8
11		188	117	8
12		206	135	8
13	(1, 3)	273	166	9
14	(3, 1)	348	195	10
15		374	221	10
16		400	247	10
17	(1, −3)	491	286	11
18	(3, −1)	590	323	12
19		624	357	12
20		658	391	12
21	(2, 3)	791	439	13
22		830	478	13
23	(3, 2)	978	528	14
24		1022	572	14

of the four linear combinations $(1, 2)$, $(2, 1)$, $(1, -2)$, and $(2, -1)$. For all values of k up to 24 it was possible to find k-sided magic dice with a set of linear combinations that contains the set of linear combinations used for $k - 1$ as a subset. We return to this point in Section 4. Table 3 shows joint probabilities for an example of 14-sided magic dice, admitting ten proper linear combinations.

TABLE 3. Joint Probabilities for 14-sided magic dice.

Columns correspond to values of X; rows to values of Y. Entries are probabilities in multiples of $1/196$. The set $\mathscr{S}$ of proper linear combinations has elements $(1,0)$, $(0,1)$, $(1,1)$, $(1,-1)$, $(1,2)$, $(2,1)$, $(1,-2)$, $(2,-1)$, $(1,3)$, and $(3,1)$.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
14	1	1	1	1	2	0	1	1	1	1	1	1	1	1
13	1	1	0	1	1	1	1	1	2	1	1	1	1	1
12	1	2	1	1	2	1	1	1	0	1	0	1	1	1
11	1	1	1	1	0	0	2	0	2	1	1	2	1	1
10	0	1	0	2	1	1	1	2	1	1	1	1	1	1
9	2	1	1	2	1	1	1	0	1	1	0	2	0	1
8	1	1	1	0	1	1	1	1	2	0	2	1	1	1
7	1	1	1	2	0	2	1	1	1	1	0	1	1	1
6	1	0	2	0	1	1	0	1	1	1	2	1	1	2
5	1	1	1	1	1	1	2	1	1	1	2	0	1	0
4	1	1	2	1	1	2	0	2	0	0	1	1	1	1
3	1	1	1	0	1	0	1	1	1	2	1	1	2	1
2	1	1	1	1	1	2	1	1	1	1	1	0	1	1
1	1	1	1	1	1	1	1	1	0	2	1	1	1	1

Our first Lemma proves two intuitively reasonable aspects of magic numbers.

Lemma 1. *For the magic numbers $m(k)$ the following holds*:

(i) $m(k+1) \geq m(k)$.
(ii) $\lim_{k\to\infty} m(k) = \infty$.

Proof: Part (i) follows by taking a matrix $\mathbf{U}$ of dimension $k \times k$ that generates k–sided magic dice, and appending a column of 1's and a row of 1's. For part (ii), we prove a stronger result that implies (ii), namely: for any set of linear combinations $\mathscr{S} = \{(a_1, b_1), \ldots, (a_p, b_p)\}$ with integer coefficients there exists a $k \in \mathbb{N}$ such that $\text{rank}[\mathbf{C}_{\mathscr{S}}] < k^2$. For any two positive integers a and b, the linear combination $aX + bY$ applied to k–sided dice can take integer values from $a + b$ to $k(a + b)$. Thus such a linear combination generates at most $(k-1)(a+b) + 1$ equations. Similarly for arbitrary integers a and b, at most $(k-1)(|a| + |b|) + 1$ equations are generated. Let $N_i = |a_i| + |b_i|$ $(i = 1, \ldots, p)$, and $N = \sum_{i=1}^{p} N_i$. Then, for k–sided dice, the set $\mathscr{S}$ generates at most

$$\sum_{i=1}^{p} [(k-1)N_i + 1] = (k-1)N + p$$

equations. Choosing k such that $k^2 > (k-1)N + p$ gives a coefficient matrix with k^2 columns and fewer than k^2 rows, which cannot have full column rank. ■

4. FINDING MAGIC NUMBERS. We now describe a simple way to compute magic numbers. Throughout this section we refer to the first and k–th rows and columns of the matrix $\mathbf{U}$ as the *margins* of $\mathbf{U}$.

Lemma 2. *For fixed k and for any $\mathscr{S} \subset \mathscr{F}_k$ the following two conditions are equivalent*:

(a) *rank*$(\mathbf{C}_{\mathscr{S}}) = k^2$.
(b) *At least one of the margins is uniquely determined.*

Proof: Clearly (a) implies (b). To show the reverse, let $\mathbf{u}_j$ be the j–th column of $\mathbf{U}$, and suppose (b) holds for the first column. Define a $k \times k$ matrix $\mathbf{U}_{-1} = (\mathbf{u}_2, \ldots, \mathbf{u}_k, \mathbf{1}_k)$, and notice that $\mathscr{S}$ generates the system of equations

$$\mathbf{C}_{\mathscr{S}} \text{vec}(\mathbf{U}'_{-1}) = \mathbf{C}_{\mathscr{S}} \mathbf{1}_{k^2}. \tag{3}$$

To see why this is true, represent the k^2 variables as grid points with coordinates $(i, j), 1 \leq i, j \leq k$, in the plane. (This is similar to the approach to be used later in the proof of Lemma 3). Each of the equations generated by $\mathscr{S}$ may be represented by a straight line that hits one or several points that correspond to variables. Formally, we may associate grid points outside the square with variables whose value is set to be 1. Then (1) holds as well if we shift the square by one unit to the right, which implies (3). By assumption, the first column vector of $\mathbf{U}_{-1}$ must be $\mathbf{1}_k$. By induction all columns of $\mathbf{U}$ must be equal to $\mathbf{1}_k$. ■

Lemma 2 shows that it is important to understand the conditions under which the margins are determined. In fact, as soon as at least one linear combination (a, b) with $ab \neq 0$ enters the equation system, some entries in the corners of $\mathbf{U}$ are determined (must take the value 1). In the next lemma, which is central to the theory, we describe the way in which the corners of $\mathbf{U}$ "fill up" as the number of linear combinations increases.

Lemma 3. *Let $\mathscr{S}^+$ be a set of $r \geq 1$ linear combinations (a_h, b_h) such that both $a_h \geq 1$ and $b_h \geq 1$. Let $a^+ = \Sigma_{h=1}^r a_h$ and $b^+ = \Sigma_{h=1}^r b_h$. If* **U** *solves the system of equations* (1) *generated by $\mathscr{S}^+$, then*

(i) *$u_{1j} = 1$ for $j = 1, \dots, a^+$, and $u_{i1} = 1$ for $i = 1, \dots, b^+$.*
(ii) *If r is even, then $u_{1, a^+ + 1} = u_{b^+ + 1, 1}$. If r is odd, then $u_{1, a^+ + 1} + u_{b^+ + 1, 1} = 2$.*
(iii) *The u_{1j} for $j > a^+$, and the u_{i1} for $i > b^+$, are not determined.*

Proof: Let $\mathscr{S}^+ = \{(a_1, b_1), \dots, (a_r, b_r)\}$. In the real plane, consider the grid given by all points with positive integer coefficients, and identify the grid point (i, j) with the corresponding variable u_{ij}. For the current purposes we may think of the number of grid points as unlimited. The linear combinations in $\mathscr{S}^+$ determine 1 to be the value of some of the variables associated with grid points near the origin. Let $m_h = a_h / b_h$ for $h = 1, \dots, k$, and assume without loss of generality that $m_1 > m_2 > \cdots > m_r$. For $h = 0, \dots, r$, let

$$\alpha_h = \sum_{i=h+1}^{r} a_i \quad \text{and} \quad \beta_h = \sum_{i=1}^{r} b_i,$$

define $r + 1$ points

$$P_h = (\beta_h + 1, \alpha_h + 1), \quad h = 0, \dots, r,$$

and call them the *characteristic points* of $\mathscr{S}^+$. In particular, we have $P_0 = (1, a^+ + 1)$ and $P_r = (b^+ + 1, 1)$. Conversely, let $P_h = (x_h, y_h)$, $h = 0, \dots, r$, denote $r + 1$ grid points in $\mathbb{N}^2$ such that $x_0 = 1$, $y_r = 1$, and the sequence $m_h = (y_{h-1} - y_h)/(x_h - x_{h-1})$ is monotonically decreasing. Then the P_h determine an associated set $\mathscr{S}^+$ with elements (a_1, b_1) to (a_r, b_r) uniquely by $P_h - P_{h-1} = (-b_h, a_h)$. Thus there is a one-to-one relationship between sets $\mathscr{S}^+$ and their characteristic points.

For a set $\mathscr{S}^+$ with characteristic points $P_0, \dots, P_r$ let l_h be the line segment connecting points P_{h-1} and P_h, and denote by $\mathscr{L}$ the polygon obtained by joining the r line segments. We now show that all variables associated with grid points inside the area bounded by $\mathscr{L}$ and the coordinate axes are determined ($= 1$) by the equations generated by $\mathscr{S}^+$. This implies part (i) of Lemma 3. See Figure 1 for a graphical illustration.

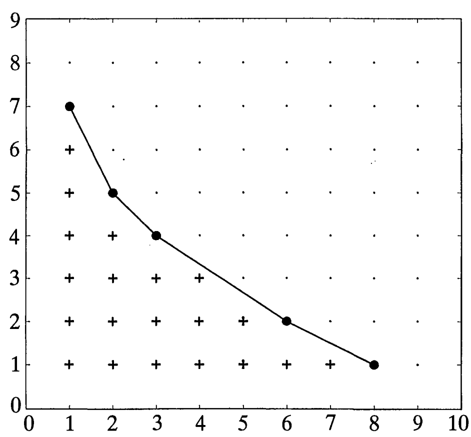


Figure 1. Illustration of the Proof of Lemma 3. Grid points whose associated variables are determined by the linear combinations in the set $\mathscr{S}^+ = \{(2, 1), (1, 1), (2, 3), (1, 2)\}$ are marked by plus-signs. The characteristic points of $\mathscr{S}^+$ are shown as large dots, and connected by the polygon $\mathscr{L}$.

We show first that the above statement implies part (ii) of Lemma 3. Denote the variables associated with the characteristic points $P_0, \ldots, P_r$ by $\xi_0, \ldots, \xi_r$. The line segment l_h corresponds to an equation $\xi_{h-1} + \xi_h = 2$ because all other grid points in $\mathbb{N}^2$ hit by the line of which l_h is a segment are determined. Thus we have an equation system

$$\begin{gathered} \xi_0 + \xi_1 = 2 \\ \xi_1 + \xi_2 = 2 \\ \vdots \\ \xi_{r-1} + \xi_r = 2 \end{gathered}$$

Successive elimination of intermediate variables gives $\xi_0 + \xi_r = 2$ if r is odd, and $\xi_0 = \xi_r$ if r is even. This proves part (ii) of Lemma 3. Note also that if we set *any* of the ξ_h equal to 1, then by the above equation system all other ξ_h are automatically 1 as well.

We now prove that all variables in the area below $\mathscr{L}$ are determined. For each real s with $1 \le s \le a^+ + 1$ let $\mathscr{L}(s)$ be the polygon obtained by translating $\mathscr{L}$ down to start at $(1, s)$ instead of at $(1, a^+ + 1)$. Let $1 = s_1 < \cdots < s_m = a^+ + 1$ be the sequence of distinct values of s such that $\mathscr{L}(s)$ passes through a grid point in the area bounded by $\mathscr{L}$ and the axes. Then, by induction on i for $i = 1$ to $i = m$, all variables are determined in the interior of the area bounded by $\mathscr{L}(s_i)$ and the axes. In passing from i to $i + 1$ it has to be shown that each grid point P on $\mathscr{L}(s_i)$ is determined. If P is the only grid point on a segment of $\mathscr{L}(s_i)$, this is obvious. If P and Q are two grid points on the same segment of $\mathscr{L}(s_i)$, they must be at the ends of the segment, s_i must be an integer, and there is a chain of grid points along $\mathscr{L}(s_i)$, one at each corner. The lowest of this chain of grid points is determined, hence so are all the others by working along the chain.

To prove part (iii), we proceed by induction on r. Assume that (iii) hold true for some $r \ge 1$, and notice that no variable associated with a grid point (i, j), where $j > a^+$, is determined. Adding a new linear combination (a_{r+1}, b_{r+1}) to the previous set $\mathscr{S}^+$ of r linear combinations, we get a new set $\mathscr{S}^+_{r+1} = \mathscr{S}^+ \cup \{(a_{r+1}, b_{r+1})\}$, whose initial characteristic point is $(1, a^+ + a_{r+1} + 1)$. The only way the variable associated with this characteristic point could be determined is that the variable associated with the point $(b_{r+1} + 1, a^+ + 1)$ is determined, which is not the case. Similarly, the variable associated with the final characteristic point of $\mathscr{S}^+_{r+1}$ is not determined. ∎

By Lemma 3, the system of equations generated by $\mathscr{S}^+$ imposes exactly $a^+ + b^+$ linearly independent constraints on the variables associated with points on the left and bottom margins: the first a^+ points are determined vertically, the first b^+ points in the margin are determined horizontally, which means that $a^+ + b^+ - 1$ points are determined around the corner, plus the additional constraint of part (ii). For fixed k, consider similarly the three remaining corners of the matrix $\mathbf{U}$. Exactly the same result as Lemma 3 is established for the corner with coordinates (k, k). For the two remaining corners, consider a set $\mathscr{S}^-$ of linear combinations (a_h, b_h) where $a_h > 0$ and $b_h < 0$, and put $a^- = \Sigma a_h$, $b^- = \Sigma |b_h|$, both sums extending over all $(a_h, b_h) \in \mathscr{S}^-$. The same arguments as in Lemma 3 show that the first a^- points are determined vertically, and the first b^- points are determined horizontally. Finally, let $\mathscr{S}^0$ be a set of linear combinations where

either $a_h = 0$ or $b_h = 0$; there are at most two elements in $\mathscr{S}^0$, each imposing a constraint on the rows and columns, respectively. Put $a^0 = \Sigma a_h$ and $b^0 = \Sigma b_h$, both sums extending over all elements in $\mathscr{S}^0$. Both a^0 and b^0 can only take values 0 and 1.

Finally, for a given set $\mathscr{S} \subset \mathscr{F}_k$, we can write $\mathscr{S}$ as the union of three disjoint sets $\mathscr{S}^0$, $\mathscr{S}^+$, and $\mathscr{S}^-$, as above. Let

$$a^* = a^0 + a^+ + a^- = \sum_{(a_h, b_h) \in \mathscr{S}} a_h$$

and

$$b^* = b^0 + b^+ + b^- = \sum_{(a_h, b_h) \in \mathscr{S}} |b_h|.$$

By the previous considerations, exactly a^* constraints exist on the first column of $\mathbf{U}$, and b^* constraints on the first row of $\mathbf{U}$. By Lemma 2, all variables in $\mathbf{U}$ are determined exactly if $a^* \geq k$ or $b^* \geq k$. If $\max\{a^*, b^*\} < k$, then $\mathbf{U}$ is not completely determined. Thus we have the following main result.

Theorem 4. *The magic number $m(k)$ is the number of elements in a largest set $\mathscr{S} \subset \mathscr{F}_k$ such that*

$$\sum_{(a_h, b_h) \in \mathscr{S}} a_h < k \quad \textit{and} \quad \sum_{(a_h, b_h) \in \mathscr{S}} |b_h| < k. \qquad \blacksquare$$

For example, the set $\mathscr{S}$ consisting of linear combinations $(1,0)$, $(0,1)$, $(1, \pm 1)$, $(1, \pm 2)$, $(2, \pm 1)$, $(1, \pm 3)$, $(3, \pm 1)$, $(2, \pm 3)$, $(3, \pm 2)$, $(1, \pm 4)$, $(4, \pm 1)$, and $(3,4)$, has 21 elements, with $\Sigma a_h = 40$, $\Sigma |b_h| = 41$. This is a largest set such that $\max\{\Sigma a_h, \Sigma |b_h|\} < 42$, and therefore $m(42) = 21$. The set is not unique because the linear combination $(3,4)$ may be replaced by any of $(3, -4)$, $(4,3)$, or $(4, -3)$. Let $\mathscr{S}^*$ be the set obtained by taking $(3,4)$ out of $\mathscr{S}$ and adding the two linear combinations $(1,5)$ and $(5,1)$; then $\mathscr{S}^*$ has 22 elements, with $\Sigma a_h = \Sigma |b_h| = 43$. This is a largest set such that $\max\{\Sigma a_h, \Sigma |b_h|\} < 44$, and therefore $m(44) = 22$. This shows that the linear combinations contained in magic k-sided dice are not necessarily all contained in magic $(k+1)$-sided dice. See the discussion following the proof of Theorem 6.

We now show how the magic number $m(k)$ can be expressed in terms of the classical Euler totient (or phi) function. For a positive integer n, $\phi(n)$ is the number of positive integers less than n that are relatively prime to n. For convenience, we define $\phi(1)$ to be 1. Also define

$$\Phi(n) = \sum_{i=1}^{n} \phi(i),$$

and

$$\Psi(n) = \sum_{i=1} i\phi(i),$$

and put $\mathscr{F} = \bigcup_{k \geq 2} \mathscr{F}_k$, where $\mathscr{F}_k$ is the feasible set for k-sided dice. For a subset $\mathscr{S}$ of $\mathscr{F}$, let $\sigma_{\mathscr{S}} = \max(\Sigma a, \Sigma |b|)$, where the sums are taken over all pairs $(a,b) \in \mathscr{S}$, and call $\mathscr{S}$ *k-bounded* if $\sigma_{\mathscr{S}} < k$. It is convenient to view $\mathscr{F}$ as an ordered

sequence of pairs in which (a, b) precedes (p, q) if

(i) $a + |b| < p + |q|$, or
(ii) $a + |b| = p + |q|$ and $||b| - a| > ||q| - p|$.

Further, if $0 < a < b < k$, with a and b relatively prime, then the pairs $(a, -b)$, $(b, -a)$, (a, b), and (b, a) appear in that order in the sequence. The first few pairs in $\mathscr{F}$, represented as an ordered sequence, are $(0, 1)$, $(1, 0)$, $(1, -1)$, $(1, 1)$, $(1, -2)$, $(2, -1)$, $(1, 2)$, $(2, 1)$, $(1, -3)$, $(3, -1)$, $(1, 3)$, $(3, 1)$, $(1, -4)$, $(4, -1)$, $(1, 4)$, $(4, 1)$, $(2, -3)$, $(3, -2)$, $(2, 3)$, $(3, 2)$, $(1, -5)$, $(5, -1), \ldots$.

For $r > 0$, define

$$\sigma_{2r} = \sum a = \sum |b|,$$

where the sums are taken over the first $2r$ pairs in the ordered sequence $\mathscr{F}$. Note that $\sigma_{2r} = \sigma_{\mathscr{S}}$ when $\mathscr{S}$ is the set of the first $2r$ elements in the ordered sequence.

Verification of the following lemma is straightforward.

Lemma 5. *If $\Phi(n) \le r < \Phi(n+1)$, then*

(i) $\sigma_{2r} = \Psi(n) + [r - \Phi(n)](n+1)$.
(ii) *Any $2r$-subset $\mathscr{S}$ of $\mathscr{F}$ must have $\sigma_{\mathscr{S}} \ge \sigma_{2r}$, and, for $r > 1$, any $(2r+1)$-subset $\mathscr{S}$ of $\mathscr{F}$ must have $\sigma_{\mathscr{S}} \ge \sigma_{2r} + \lfloor (n+3)/2 \rfloor$.* ■

Trivially, $m(2) = 2$ and $m(3) = 3$. For $k > 3$, Lemma 5 enables us to establish the value of $m(k)$.

Theorem 6. *For $k > 3$, suppose $\Psi(n) < k \le \Psi(n+1)$, and let $p = k - \Psi(n) - 1$.*

(i) *If $p \bmod (n+1) < \lfloor (n+3)/2 \rfloor$, then*

$$m(k) = 2\Phi(n) + 2\lfloor p/(n+1) \rfloor,$$

and a maximum cardinality k-bounded subset of $\mathscr{F}$ can be obtained by taking the first $m(k)$ pairs in the ordered sequence.

(ii) *If $p \bmod (n+1) \ge \lfloor (n+3)/2 \rfloor$, then*

$$m(k) = 2\Phi(n) + 2\lfloor p/(n+1) \rfloor + 1,$$

and a maximum cardinality k-bounded subset of $\mathscr{F}$ can be obtained by taking the first $m(k) - 1$ pairs in the ordered sequence together with the pair $(\lfloor (n+3)/2 \rfloor, \lfloor (n+1)/2 \rfloor)$.

Proof: (i) If $r = \Phi(n) + \lfloor p/(n+1) \rfloor$, then by Lemma 5(i),

$$\sigma_{2r} = \Psi(n) + (n+1)\lfloor p/(n+1) \rfloor \le \Psi(n) + p = k - 1,$$

so we have a k-bounded set of the claimed size. On the other hand, by Lemma 5(ii), any subset $\mathscr{S}$ of $\mathscr{F}$ of size $\ge 2r + 1$ has

$$\begin{aligned} \sigma_{\mathscr{S}} &\ge \sigma_{2r} + \lfloor (n+3)/2 \rfloor \\ &= \Psi(n) + (n+1)\lfloor p/(n+1) \rfloor + \lfloor (n+3)/2 \rfloor \\ &> \Psi(n) + p - \lfloor (n+3)/2 \rfloor + \lfloor (n+3)/2 \rfloor \\ &= k - 1, \end{aligned}$$

and so it cannot be k-bounded.

(ii) If $r = \Phi(n) + \lfloor p/(n+1) \rfloor$, then, if $\mathscr{S}$ is the set described, Lemma 5(i) gives

$$\begin{aligned}\sigma_{\mathscr{S}} &= \sigma_{2r} + \lfloor (n+3)/2 \rfloor \\ &= \Psi(n) + (n+1)\lfloor p/(n+1) \rfloor + \lfloor (n+3)/2 \rfloor \\ &\le \Psi(n) + p - \lfloor (n+3)/2 \rfloor + \lfloor (n+3)/2 \rfloor \\ &= k-1,\end{aligned}$$

so again we have a k-bounded set of the claimed size. On the other hand, it is easy to verify that

$$\sigma_{2r+2} \ge \sigma_{2r} + n + 1,$$

so that, by Lemma 5(ii), any subset $\mathscr{S}$ of $\mathscr{T}$ of size $\ge 2r+2$ has

$$\begin{aligned}\sigma_{\mathscr{S}} &\ge \sigma_{2r+2} \\ &\ge \Psi(n) + (n+1)\lfloor p/(n+1) \rfloor + n + 1 \\ &\ge \Psi(n) + p - (p \bmod (n+1)) + n + 1 \\ &> k-1,\end{aligned}$$

and so cannot be k-bounded. ∎

As seen from Theorem 6, a set of k-sided magic dice can not always be constructed such as to contain the same linear combinations as magic $(k-1)$-sided dice. Theorem 6 allows us also to establish the asymptotic behavior of the function $m(k)$, based on the growth rate of the function Φ. First we need another preliminary lemma.

Lemma 7. *For the functions $\Phi(n)$ and $\Psi(n)$, the following holds*:

(i) $\Phi(n) = 3n^2/\pi^2 + O(n \log n)$.
(ii) $\Psi(n) = 2n^3/\pi^2 + O(n^2 \log n)$.

Proof: For part (i), see [3, pp. 448–449]. For part (ii), by summation of parts, $\Psi(n) = n\Phi(n) - \sum_{i=1}^{n-1}\Phi(i)$. Thus

$$\Psi(n) = \frac{3}{\pi^2}n^3 + O(n^2 \log n) - \frac{3}{\pi^2}\sum_{i=1}^{n-1}\left[i^2 + O(i \log i)\right],$$

and the result follows. ∎

Theorem 8. *The asymptotic behavior of $m(k)$ is*

$$m(k) = ck^{2/3} + O(k^{1/3}\log k), \quad \text{where } c = 6/(2\pi)^{2/3} \approx 1.7621.$$

Proof: Given k, choose n such that

$$\Psi(n) < k \le \Psi(n+1),$$

and hence

$$2\Phi(n) = m(\Psi(n)+1) \le m(k) < m(\Psi(n+1)+1) = 2\Phi(n+1).$$

From Lemma 7(ii) we have

$$k = \frac{2}{\pi^2}n^3 + O(n^2 \log n),$$

and from Lemma 7(i),

$$m(k) = \frac{6}{\pi^2}n^2 + O(n\log n).$$

It follows that

$$n = \left(\pi^2/2\right)^{1/3} k^{1/3} + O(\log n)$$

and so

$$m(k) = \frac{6}{\pi^2}\left[\left(\pi^2/2\right)^{1/3} k^{1/3} + O(\log n)\right]^2 + O(n\log n).$$

Using $n = O(k^{1/3})$ leads to the stated result. ■

Figure 2 shows a graph of exact values of $m(k)$ along with the approximation $\hat{m}(k) = 6k^{2/3}/(2\pi)^{2/3}$, for $2 \le k \le 100$. As can be seen from the graph, the approximation is excellent.

Before you ask, the magic number for 1998–sided dice is 280.

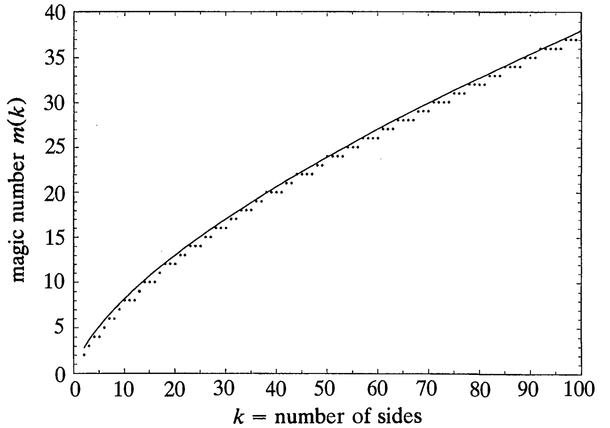


Figure 2. Exact values of the magic function $m(k)$ (dots) and approximation $\hat{m}(k) = 6k^{2/3}/(2\pi)^{2/3}$ (solid line).

5. THE RANK OF THE COEFFICIENT MATRIX. The theory of Section 4 allows us to find the magic number $m(k)$ as well as an associated set $\mathscr{S} \subset \mathscr{F}$ without solving the equation system of Section 3. For generating actual magic dice we still have to solve the equation system. As a byproduct of the Gauss–Jordan algorithm we obtain the rank of the coefficient matrix $\mathbf{C}_{\mathscr{S}}$. In the current section we give a simplified method for computing the rank of $\mathbf{C}_{\mathscr{S}}$ that does not require solving the equation system.

The idea is to study how the rank increases for a given set $\mathscr{S}$ of linear combinations if we go from $(k-1)$–sided dice to k–sided dice. Let $\mathbf{U}$ be the $(k-1) \times (k-1)$ matrix of variables for $(k-1)$–sided dice, and write $\mathbf{A}$ (instead of $\mathbf{C}_{\mathscr{S}}$ as before) for the coefficient matrix generated by the linear combinations in $\mathscr{S}$. Going from $k-1$ to k, we add a row and a column to the matrix $\mathbf{U}$, thus introducing $2k-1$ new variables to get a new matrix $\mathbf{U}^*$ of dimension $k \times k$. Instead of writing the equation system for k–sided dice in terms of vec($\mathbf{U}^{*\prime}$) as before, consider the variables contained in $\mathbf{U}$ as the $(k-1)^2$ first ones, and the

$2k - 1$ new variables as the last ones. The coefficient matrix for k-sided dice can then be written in partitioned form as

$$\mathbf{A}^* = \begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{O} & \mathbf{C} \end{bmatrix}.$$

If $\mathbf{A}$ has s rows, then $\mathbf{B}$ has dimension $s \times (2k - 1)$. That is, the entries of $\mathbf{B}$ are coefficients of the newly introduced variables, but only for equations that involve entries from $\mathbf{U}$. The matrix $\mathbf{C}$ contains the coefficients of all equations that involve only newly introduced variables; it has $2k - 1$ columns and $\Sigma(a_h + |b_h|)$ rows. We will now show how $r(k-1; \mathscr{S}) = \operatorname{rank}(\mathbf{A})$ and $r(k; \mathscr{S}) = \operatorname{rank}(\mathbf{A}^*)$ are related.

Perform Gauss–Jordan type row operations on the matrix $\mathbf{A}^*$, based on the first $(k-1)^2$ columns, until as many rows as possible have zeros in the first $(k-1)^2$ entries. That is, transform $\mathbf{A}^*$ into

$$\begin{bmatrix} \mathbf{A}_1 & \mathbf{B}_1 \\ \mathbf{O} & \mathbf{B}_2 \\ \mathbf{O} & \mathbf{C} \end{bmatrix},$$

where $\mathbf{A}_1$ has full row rank $r(k-1; \mathscr{S})$. Because $\mathbf{A}_1$ has full row rank, we get

$$\operatorname{rank}(\mathbf{A}^*) = \operatorname{rank}(\mathbf{A}_1) + \operatorname{rank}\begin{bmatrix} \mathbf{B}_2 \\ \mathbf{C} \end{bmatrix}.$$

Thus the rank of the coefficient matrix increases by $\delta = \operatorname{rank}\begin{bmatrix} \mathbf{B}_2 \\ \mathbf{C} \end{bmatrix}$ when going from $(k-1)$-sided dice to k-sided dice. But δ is the number of linearly independent constraints imposed on the newly introduced variables, i.e., the number of constraints imposed by $\mathscr{S}$ on the variables in the first row and first column, say, of the matrix $\mathbf{U}^*$.

In the notation and terminology of Section 4, consider the lower left corner of a $k \times k$ grid, and assume $\max\{\Sigma a_h, \Sigma |b_h|\} < k$, where both sums extend over all elements in $\mathscr{S}$. By Lemma 3, the variables associated with $a^+ + b^+ - 1$ grid points around the corner $(1,1)$ are determined. In addition, there is a linear constraint between one of the variables in the first column and one of the variables in the first row, making the total number of constraints due to $\mathscr{S}^+$ equal to $a^+ + b^+$. The linear combinations in $\mathscr{S}^-$ determine another a^- variables vertically and b^- variables horizontally, and the linear combinations in $\mathscr{S}^0$ add a^0 and b^0 constraints vertically and horizontally, respectively. Thus the total number of constraints is $\Sigma(a_h + |b_h|)$, where the sum extends over all elements in $\mathscr{S}$. The rank increase is therefore $\delta = \Sigma(a_h + |b_h|)$, independent of k, as long as k is large enough.

If either $\Sigma a_h \geq k$ or $\Sigma |b_h| \geq k$, then Lemma 2 ensures that $\operatorname{rank}(\mathbf{A}) = (k-1)^2$ and $\operatorname{rank}(\mathbf{A}^*) = k^2$; that is, the rank increase is $\delta = 2k - 1$. Finally, notice that for $k = 1$ the rank of the coefficient matrix is always 1, regardless of how many linear combinations are in $\mathscr{S}$.

This is summarized in the following theorem.

Theorem 9. *Let $r(k; \mathscr{S})$ denote the rank of the coefficient matrix of the equation system generated by the linear combinations (a_h, b_h) in the set $\mathscr{S}$, for k-sided dice. Then, for $k \geq 2$,*

$$r(k; \mathscr{S}) = \begin{cases} r(k-1; \mathscr{S}) + \Sigma(a_h + |b_h|) & \text{if } \max\{\Sigma a_h, \Sigma |b_h|\} < k, \\ k^2 & \text{otherwise}. \end{cases} \qquad \blacksquare$$

For a given set $\mathscr{S}$ of linear combinations, Theorem 9 provides a simple recursion to compute the rank of the coefficient matrix. In particular, if $\mathscr{S}$ is a largest set of proper linear combinations, then $r(k; \mathscr{S}) = (k-1)^2 + \Sigma(a_h + |b_h|)$, and the number of free variables in the equations system is $2k - \Sigma(a_h + |b_h|) - 1$. For instance, in Section 4 we gave a set $\mathscr{S}$ of linear combinations for 42–sided magic dice and found $m(42) = 21$. Theorem 9 gives $r(42; \mathscr{S}) = 1762 = 42^2 - 2$. For all sets of 1998–sided magic dice, the rank is $3992003 = 1998^2 - 1$.

Finally, we return to a question raised in Section 3: Is it always possible to find an integer–valued solution to the system of equations generated by $\mathscr{S}$? The answer is yes, by the following argument. If the coefficient matrix has rank r, then the values of $f = k^2 - r$ variables can be chosen. Identify a free variable associated with a characteristic point. Set the remaining (if any) $f - 1$ free variables equal to 1, and assign the value 0 or 2 to the chosen free variable. Then, working along chains like the polygon in Figure 1, variables are assigned values of 2 and 0 in an alternating pattern.

6. EPILOGUE. "Magic Dice" originated in the first author's attempts to teach undergraduate students that marginal distributions do not determine joint distributions. It is natural to ask how much more information needs to be given (in addition to the marginal distributions) such that a joint distribution is completely determined. Although the story about the magician is flawed (in the sense that it appears physically impossible to construct such dice), students can relate to it and find it entertaining. In fact, it would take a TRUE magician to make the numbers shown by two dice depend on each other! This distinguishes our magic dice (or "pseudo dice," as suggested by a reviewer), from tricks with dice as described in **[2]**. The term "magic" may also be justified by the similarities with magic squares **[6]**.

The idea of defining a joint distribution of two or several random variables by conditions imposed on linear combinations of the variables is not new; for example, a common definition of the multivariate normal distribution states that $\mathbf{X}$ is multivariate normal if every linear combination of $\mathbf{X}$ is univariate normal or constant. Melnick and Tenenbein give a nice example to illustrate that for any finite k, normality of k linear combinations does not imply multivariate normality **[4]**. For the discrete case, Rényi shows that a distribution of n strictly positive masses located at n distinct points in the plane, where both the sizes and locations of the masses are unknown, is determined by any $n + 1$ distinct projections, but not necessarily by n distinct projections **[5]**. Bélisle et al. study related questions for non–discrete probability distributions **[1]**.

Finally, it is not difficult to see that the same results hold as well for arbitrary distributions on a $k \times k$ grid, as long all k^2 probabilities are strictly positive. Up to Theorem 4, results also generalize easily to the situation of distributions on a rectangular grid of size $k_1 \times k_2$. It is natural to ask related questions in higher dimension, but to our knowledge no results have appeared in the literature.

REFERENCES

1. Bélisle, C., Massé, J.–C., and Ransford, T., When is a probability measure determined by infinitely many projections? *Ann. Prob.* **25** (1997) 767–786.
2. Gardner, M., *Mathematics, Magic and Mystery*, Dover, New York, 1956.
3. Graham, R. L., Knuth, D. E., and Patashnik, O., *Concrete Mathematics*, Addison–Wesley, 1989.

4. Melnick, E. L., and Tenenbein, A., Misspecifications of the normal distribution. *Amer. Statist.* **36** (1982) 372–373.
5. Rényi, A., On projections of probability distributions. *Acta Math. Hungar.* **3** (1952) 131–142.
6. Ward, J. E., Vector spaces of magic squares. *Math. Mag.* **53** (1980), 108–111.

BERNARD D. FLURY studied statistics and mathematics at the University of Berne, Switzerland. After a random walk around the world he became Professor of Statistics in the Department of Mathematics, Indiana University. His research focuses on theoretical, practical, and computational aspects of multivariate statistics, mostly related to problems in classification and principal component analysis. Other research interests include beer and frequent trips to Italy.
Indiana University, Bloomington, IN 47405
flury@indiana.edu

ROBERT IRVING completed his BSc and PhD degrees in mathematics at the University of Glasgow in Scotland. After periods as a communications specialist and as a lecturer in mathematics and computer science at Salford University in Manchester, he returned to the Computing Science Department at Glasgow where he is now a Senior Lecturer. His research interests are in the areas of algorithms and complexity theory, including combinatorial optimization, graph theory, and "stringology."
Computing Science Department, University of Glasgow, Glasgow G12 8QQ, Scotland
rwi@dcs.gla.ac.uk

M. N. GORIA completed his MA in statistics at the University of Punjab (Lahore, Pakistan), and his PhD in statistics at the University of California in Berkeley. He is now Professor of Statistics at the University of Trento. His research focuses on parametric and nonparametric statistical inference.
Istituto di Statistica e Ricerca Operativa, Università degli Studi di Trento, Via Inama, 38100 Trento, Italy
mgoria@gelso.unitn.it

It's a kind of transitive law, isn't it?
when, in a house of growing children
two people who pet the same cat are petting each other.
Especially if one of them is holding the cat.
Especially if both of them are holding the cat.
And if Devin gets under the blanket with Mirage
and lets only their heads stick out
and smiles up in that way
if the pug of his nose is close to that spot between Mirage's ears
and if I grab hold of it all
and kiss it all . . .

well, Devin also knows
and Mirage also knows
that something is necessary
something is sufficient
and something else is scared.

Contributed by Marion Cohen, Drexel University, Philadelphia, PA

The Set of Differences of a Given Set

Andrew Granville and Friedrich Roesler

1. INTRODUCTION. A central problem of combinatorial geometry and additive number theory is to understand the set of sums or differences of a given set of vectors. For example, given a set of m arbitrary vectors A, how big is the set $A + A := \{a + b\colon a, b \in A\}$, or the set $A - A := \{a - b\colon a, b \in A\}$? By packing the vectors close together on a lattice one can make these sets small: for example, if $A = \{a, 2a, 3a, \dots, (m-1)a, ma\}$ then $A + A$ and $A - A$ both have $2m - 1$ elements. On the other hand, if the elements of A are appropriately spread out then we can make these sets large: for example, if $A = \{2^1, 2^2, \dots, 2^m\}$ then $A + A$ has $(m^2 + m)/2$ elements, and $A - A$ has $m^2 - m + 1$ elements.

It may be that the sizes of $A - A$ and $A + A$ are quite different: For example if A is the set of positive integers smaller than 10^k that have only digits 1, 2, and 4 in their decimal expansions then A has 3^k elements and $A + A$ has 6^k elements, far smaller than $A - A$, which has 7^k elements. Similarly, one can construct A so that $A + A$ is far larger than $A - A$, for example by taking $A = \sum_{i=0}^{k-1} b_i 100^i$ where each b_i is allowed to take any value from the set $\{0, 2, 3, 4, 7, 11, 12, 14\}$; see **[7]** and **[8]** for more details. For the more natural example $A = \{1^2, 2^2, \dots, n^2\}$ it can be shown, though with some difficulty, that $A - A$ is about $\log^{\kappa} n$ times as large as $A + A$, for some constant $\kappa > 0$.

Some time ago it was realized that if either $A + A$ or $A - A$ is very small then A must have some special structure: Indeed, Freiman **[5]** (but see **[9]**) showed that A must then be a subset of a small part of a lattice. There have recently been several striking and elegant advances in this area of combinatorial additive number theory; see **[1]**, **[2]**, and **[6]**. Moreover Gowers has recently given a spectacular application of Freiman's theorem, which proves the first reasonable upper bounds in Szemerédi's theorem: Given a positive integer k and a $\delta > 0$, every subset of $\{1, 2, \dots, n\}$ with at least δn elements contains a k-term arithmetic progression, provided $n > N(k, \delta)$. Gowers gave the upper bound **[13]**

$$N(k, \delta) \le 2^{2^{|\log \delta|^{2^{c \cdot 2^k}}}},$$

for some constant c, a substantial improvement over bounds known previously.

Seemingly unrelated to all this is

Graham's conjecture. *For any set A of m distinct positive integers, we have*

$$\max_{a, b \in A} \frac{a}{\gcd(a, b)} \ge m.$$

Equality holds only in the following cases:

- $A = \{2, 3, 4, 6\}$.
- $A = \{k, 2k, \dots, mk\}$ *for some integer* k.
- $A = \{l/1, l/2, \dots, l/m\}$ *for some integer l divisible by the least common multiple of* $1, \dots, m$.

This old chestnut has recently been proved correct in an outstandingly original, though long and complicated, paper by Balasubramanian and Soundararajan **[3]**. Their method involves very careful consideration of prime divisors of linear combinations of numbers from A. In fact Graham's conjecture had been elegantly proved for sufficiently large m by Szegedy **[10]** and Zaharescu **[12]** a decade earlier, but it took a wealth of new ideas to extend their result to all integers m.

In search of a more combinatorial proof, one might approach Graham's conjecture by asking whether there are at least m distinct integers in the set $\{a/\gcd(a,b)\colon a, b \in A\}$? If so, Graham's conjecture would follow easily. Unfortunately the answer is "no," since for

$$A = \{2,3,4,6,9,12,18\} \tag{1}$$

one gets the set $\{1,2,3,4,6,9\}$.

Unsolved problem. *For each integer $m \geq 1$, what is the least number of integers one can have in the set $\{a/\gcd(a,b)\colon a,b \in A\}$, where A is a set of m distinct positive integers?*

One can relate this problem quite closely to the vector questions asked at the beginning of the Introduction:

Let $p_1, p_2, \ldots, p_n$ be the set of primes that divide integers in A. Write each $a \in A$ in the form $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and associate to it the vector $\mathbf{a} = (a_1, \ldots, a_n)$; note that distinct integers are associated with different vectors. Now, given $a, b \in A$, evidently $\min\{a_i, b_i\}$ is the ith component of the vector associated with $\gcd(a,b)$. Thus $a_i - \min\{a_i, b_i\} = \max\{0, a_i - b_i\}$ is the ith component of the vector associated with $a/\gcd(a,b)$; we call this vector $\delta(\mathbf{a},\mathbf{b})$. Thus we have:

Unsolved problem (restated). *For each integer $m \geq 1$, what is the least number of vectors one can have in the set $\delta(A) := \{\delta(\mathbf{a},\mathbf{b}) : \mathbf{a}, \mathbf{b} \in A\}$, where A is a set of m distinct vectors?*

Remark. We can claim that this is a restatement of the first unsolved problem only if we state that the vectors in A all have non-negative integer entries. However, through a few minor technical tricks one can drop that requirement; we leave this as a challenge to the reader.

To get the lower bound $|\delta(A)| \geq m^{1/2}$ in the unsolved problem, we first note that, for fixed $\mathbf{a} \in A$, the pairs $(\delta(\mathbf{a},\mathbf{b}), \delta(\mathbf{b},\mathbf{a}))$ must all be distinct since $\mathbf{b} = \mathbf{a} - \delta(\mathbf{a},\mathbf{b}) + \delta(\mathbf{b},\mathbf{a})$, and so there are no less than m distinct pairs. Thus there are either $\geq m^{1/2}$ distinct values for $\{\delta(\mathbf{a},\mathbf{b}) : \mathbf{b} \in A\}$ or for $\{\delta(\mathbf{b},\mathbf{a}) : \mathbf{b} \in A\}$, else there would be less than m distinct pairs $(\delta(\mathbf{a},\mathbf{b}), \delta(\mathbf{b},\mathbf{a}))$, giving a contradiction.

One can get a better lower bound for $\delta(A)$ if A is a set of vectors in the plane:

Theorem 1. *If $A \subset \mathbb{R}^2$ is a set of $m \geq 1$ distinct vectors then $\delta(A)$ has at least $(m/2)^{2/3}$ vectors. In fact there exists $\mathbf{a} \in A$ such that there are at least $(m/2)^{2/3}$ distinct vectors amongst $\{\delta(\mathbf{b},\mathbf{a}) : \mathbf{a} \in A\}$.*

Perhaps such a lower bound holds in higher dimension. We postpone the proof of this and other results until subsequent sections.

The example given in (1) is a translation of the set $A = \{(x,y) \in \mathbb{Z}^2 : 0 \leq x, y \leq 2, 1 \leq x + y \leq 3\}$, given by Freiman and Lev (taking $n = 2, p_1 = 2, p_2 = 3$). They generalized this to $A = \{(x,y) \in \mathbb{Z}^2 : x, y \geq 0, L < x + y \leq U\}$ with $L = ((2m)^{2/3} - (2m)^{1/3})/2 + O(1)$ and $U = ((2m)^{2/3} + (2m)^{1/3})/2 + O(1)$. Then

$\delta(A)=\{(x,y)\in\mathbb{Z}^2 : x,y\geq 0, x+y<U-L\}\cup\{(t,0),(0,t)\in\mathbb{Z}^2 : 0\leq t\leq U\}$, which has $\sim(3/2)(2m)^{2/3}$ elements. Thus the lower bound in Theorem 1 is best possible up to a factor of $3\cdot 2^{1/3}$. Moreover from these remarks, combined with those directly above the statement of Theorem 1, we obtain the following partial result concerning our unsolved problem:

Theorem 2. *If A is any set of $m\geq 1$ distinct vectors with $|\delta(A)|$ minimal, then* $(3/2)(2m)^{2/3}\gtrsim|\delta(A)|\geq m^{1/2}$.

The function $a/\gcd(a,b)$ in the unsolved problem is not symmetric in a and b. It thus might seem more natural to study the number of distinct values in $\{ab/\gcd(a,b)^2 : a,b\in A\}$. In this case we can prove a best possible result:

Theorem 3. *For any set of natural numbers A, there are at least $|A|$ natural numbers in the set $\{ab/\gcd(a,b)^2 : a,b\in A\}$.*

Remark. We show in Section 3 that the proof of Theorem 4 (which implies Theorem 3) can be modified to prove that equality holds only for the following sets A: Let $q_1,q_2,\ldots,q_k$ be positive rational numbers, with each $q_i=r_i/s_i\neq 1$ and $\gcd(r_i,s_i)=1$ such that $\gcd(r_is_i,r_js_j)=1$ if $i\neq j$. Let S be a subgroup of $(\mathbb{Z}/2\mathbb{Z})^k$. Then A is the set of integers $bq_1^{i_1}q_2^{i_2}\cdots q_k^{i_k}$ where the i_j satisfy $l_j\leq i_j\leq u_j$, for some lower and upper bounds l_j and u_j, with $(i_1,i_2,\ldots,i_k)\in S$, and b chosen so that these numbers are indeed all integers.

A simple example is when $A=\{d : d|n\}$ for any positive integer n. A more exotic example is $A=\{md^2 : d|n, m=1 \text{ or } b\}$ where squarefree $b>1$ divides n.

We may rewrite the question in Theorem 3 as a problem about sets of vectors: The ith component of the vector, $d(\mathbf{a},\mathbf{b})$, associated with $ab/\gcd(a,b)^2$ is

$$a_i+b_i-2\min\{a_i,b_i\}=|a_i-b_i|.$$

Therefore

$$d(\mathbf{a},\mathbf{b})=\delta(\mathbf{a},\mathbf{b})+\delta(\mathbf{b},\mathbf{a})=(|a_1-b_1|,|a_2-b_2|,\ldots,|a_n-b_n|)$$

since $\mathbf{a}-\mathbf{b}=\delta(\mathbf{a},\mathbf{b})-\delta(\mathbf{b},\mathbf{a})$. Thus Theorem 3 is equivalent to the following result (which we shall prove in the next section):

Theorem 4. *If A is a finite set of distinct vectors in $\mathbb{R}^n$ then $D(A)=\{d(\mathbf{a},\mathbf{b}) : \mathbf{a},\mathbf{b}\in A\}$ has at least as many distinct vectors as A.*

These vector questions may all be thought of as problems about the set of distinct differences $\{\Delta(\mathbf{a},\mathbf{b}) : \mathbf{a},\mathbf{b}\in A\}$ for some naturally defined "difference" function Δ between two vectors. Moreover, each of our questions has a number theoretic interpretation; the set of values $\{\mathbf{a}-\mathbf{b}\}$ corresponds simply to looking at all ratios a/b of the corresponding integers. It is perhaps of interest to consider other difference functions that relate elementary number theory to vector problems, though we have been unable to identify any others that are particularly appealing:

Perhaps the most obvious difference function between two vectors is the Euclidean distance, $(|a_1-b_1|^2+|a_2-b_2|^2+\cdots+|a_n-b_n|^2)^{1/2}$. Unfortunately there is no straightforward number theoretic interpretation for the associated problem about integers. Moreover any set of orthonormal vectors has the property that the set of distances between pairs of vectors is $\{0,1\}$. However, Erdős **[4]** restricted his attention to a set A of m distinct points in the plane. He noted that

for the points in the k-by-k integer lattice, where $k = \sqrt{m} + O(1)$, we have $\#\{|\mathbf{a}-\mathbf{b}| : \mathbf{a}, \mathbf{b} \in A\} \sim cm/\sqrt{\log m}$ for some constant $c > 0$, and asked whether this is best possible, up to the value of c? The best result in this direction, due to Székely **[11]**, is that there exists some $\mathbf{b} \in A$ such that $\#\{|\mathbf{a}-\mathbf{b}| : \mathbf{a} \in A\} \geq c'm^{4/5}$, for some constant $c' > 0$.

2. PROOFS OF THE THEOREMS. Although we found several proofs of Theorem 1, we decided to present here the following elegant proof communicated to us by Sudakov:

Proof of Theorem 1 (Sudakov). Let x_1 be the smallest element of $X = \{x : (x, y) \in A\}$, the x-coordinates of points in A, and let $Y = \{y : (x, y) \in A\}$, the y-coordinates of points in A. Then $\delta(A)$ contains points with x-coordinate $x - x_1$ for each $x \in X$, so $|\delta(A)| \geq |X|$ (and therefore we take $\mathbf{a}$ to be any element of A with x-coordinate equal to x_1) . Similarly $|\delta(A)| \geq |Y|$. Thus our result is proved true unless $|X|, |Y| < (m/2)^{2/3}$, which we now assume.

We define a series of sets $A_1 = A \supset A_2 \supset \cdots \supset A_k$, and then let L_i be the set of *lines* of A_i, that is, the sets of points $\{(x, y) \in A_i\}$ for each $x \in X_i := \{x : (x, y) \in A_i\}$, and the sets of points $\{(x, y) \in A_i\}$ for each $y \in Y_i := \{y : (x, y) \in A_i\}$. The average number of points on each line in L_i is $r_i : = 2|A_i|/(|X_i| + |Y_i|)$. Suppose there is a line in L_i that has less than $r_i/2$ points; we obtain the set A_{i+1} by removing the points of that line from the set A_i. Notice that $r_i < r_{i+1}$. We continue with this process until we reach the set A_k, in which every line in L_k has at least $r_k/2 \geq r_1/2 = m/(|X| + |Y|) \geq (m/2)^{1/3}$ points.

Let x_0 be the smallest element of X_k. Let y_0 be the smallest element of $Y_0 = \{y : (x_0, y) \in A_k\}$, a set that is the same size as the line $\{(x_0, y) : y \in Y_0\}$ of A_k and hence has size at least $(m/2)^{1/3}$. Let $B \subset A_k \subset A$ be the union, over each $y \in Y_0$, of the lines $\{(x, y) \in A_k\}$ of L_k. Each of these lines contains at least $(m/2)^{1/3}$ elements, so that B has at least $(m/2)^{2/3}$ elements. Now $\delta(\mathbf{b}, (x_0, y_0)) = \mathbf{b} - (x_0, y_0)$ for each $\mathbf{b} \in B$, so that these δ values are distinct. Therefore $|\delta(A)| \geq |\delta(B)| \geq |B|$ (and $\mathbf{a} = (x_0, y_0)$). ∎

Proof of theorem 4 We use induction on n and then on the size of the set A. If A has just one element then $D(A)$ contains only the zero vector, and so has exactly as many distinct vectors as A. If $n = 1$ and $A = \{a_1 < a_2 < a_3 < \cdots < a_m\}$ then $\{0, a_2 - a_1, a_3 - a_1, \ldots, a_m - a_1\} \subseteq D(A)$. This subset of $D(A)$ has exactly as many distinct vectors as A, so $|D(A)| \geq |A|$.

We may now assume that $|A| > 1$ and $n > 1$. Define

$$B = \{(x_1, \ldots, x_{n-1}) : \text{ there exists } x_n \text{ with } (x_1, \ldots, x_{n-1}, x_n) \in A\},$$

the projection of A onto the first $n - 1$ dimensions. Since B is a finite, non-empty set of distinct vectors in $\mathbb{R}^{n-1}$, we can invoke the induction hypothesis to obtain

$$|D(B)| \geq |B|. \tag{2}$$

Now, for each $\mathbf{b} \in B$, let

$$A_{\mathbf{b}} = \{x_n : (\mathbf{b}, x_n) \in A\} \text{ and let } a_{\mathbf{b}} = \max\{x : x \in A_{\mathbf{b}}\},$$

so $A_{\mathbf{b}}$ is the set of numbers that give the nth coordinate of a vector in A when appended to the $n - 1$ coordinates of $\mathbf{b}$, and $a_{\mathbf{b}}$ is the largest such number. Finally, let $C = A - \{(\mathbf{b}, a_{\mathbf{b}}) : \mathbf{b} \in B\}$. That is, we get C by removing exactly one vector from A for each $\mathbf{b} \in B$, namely the vector $(\mathbf{b}, a_{\mathbf{b}})$; in other words by "skimming off the highest point which projects onto $\mathbf{b}$, for each $\mathbf{b} \in B$." Therefore

$$|C| = |A| - |B|. \tag{3}$$

Since $|C| < |A|$ we deduce, from the induction hypothesis, that

$$|D(C)| \geq |C|. \tag{4}$$

We may describe $D(A)$ and $D(C)$ in terms of the elements of $D(B)$ and the elements of the sets $A_{\mathbf{b}}$:

$$D(A) = \cup_{D \in D(B)} \{(D, |a - a'|) : d(\mathbf{b}, \mathbf{b}') = D \text{ with } a \in A_{\mathbf{b}} \text{ and } a' \in A_{\mathbf{b}'}\}.$$

Similarly, since $C_{\mathbf{b}} = A_{\mathbf{b}} - \{a_{\mathbf{b}}\}$, we obtain

$$D(C) = \cup_{D \in D(B)} \{(D, |c - c'|) : d(\mathbf{b}, \mathbf{b}') = D \text{ with } c \in C_{\mathbf{b}} \text{ and } c' \in C_{\mathbf{b}'}\}.$$

Now comes the key observation in our argument: For any pair $\mathbf{b}, \mathbf{b}' \in B$, the largest difference $|a - a'|$ with $a \in A_{\mathbf{b}}$ and $a' \in A_{\mathbf{b}'}$, must have $a = a_{\mathbf{b}}$ or $a' = a_{\mathbf{b}'}$. Thus this largest difference does not appear among the set of differences $\{|c - c'| : c \in C_{\mathbf{b}}, c' \in C_{\mathbf{b}'}\}$. We deduce that, for any $D \in D(B)$, the set

$$\{|c - c'| : d(\mathbf{b}, \mathbf{b}') = D \text{ with } c \in C_{\mathbf{b}} \text{ and } c' \in C_{\mathbf{b}'}\}$$

does not contain the largest element of

$$\{|a - a'| : d(\mathbf{b}, \mathbf{b}') = D \text{ with } a \in A_{\mathbf{b}} \text{ and } a' \in A_{\mathbf{b}'}\},$$

so it is a proper subset, and is thus smaller. Comparing the sizes of $D(A)$ and $D(C)$, and taking this observation into account, we obtain

$$\begin{aligned} |D(C)| &\leq \sum_{D \in D(B)} \left(\#\{|a - a'| : d(\mathbf{b}, \mathbf{b}') = D \text{ with } a \in A_{\mathbf{b}} \text{ and } a' \in A_{\mathbf{b}'}\} - 1\right) \\ &\leq |D(A)| - |D(B)|. \end{aligned} \tag{5}$$

Combining (2), (3), (4), and (5) gives

$$|D(A)| \geq |D(B)| + |D(C)| \geq |B| + |C| = |A|,$$

as required.

3. WHEN DOES EQUALITY HOLD IN THEOREM 4? As we indicated at the beginning of the Introduction, equality typically holds in inequalities such as Theorem 4, only when the vectors in A form part of a lattice. Let $\mathbb{I}_k$ be the set of all subsets I of $\mathbb{Z}^k$ of the form $R \cap \Lambda$, where R is some rectangular box with sides parallel to the axes, and Λ is a lattice with $(2\mathbb{Z})^k \subseteq \Lambda \subseteq \mathbb{Z}^k$. More specifically the points $(i_1, i_2, \dots, i_k) \in S$, with each i_j contained in some interval $[l_j, u_j]$, and S a subgroup of $(\mathbb{Z}/2\mathbb{Z})^k$. One can easily verify that equality holds in Theorem 4 for any $A \in \mathbb{I}_k$; in fact equality holds if and only if A is a suitable translation of some $I \in \mathbb{I}_k$:

Proposition 1. *If $A \subset \mathbb{R}^n$ with $|D(A)| = |A|$ then there exist $\mathbf{a}, \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k \in \mathbb{R}^n$, with the gth component of $\mathbf{v}_j$ non-zero for at most one j for each g, such that $A = \{\mathbf{a} + \sum_{j=1}^k i_j \mathbf{v}_j : (i_1, i_2, \dots, i_k) \in I\}$, where $I \in \mathbb{I}_k$.*

Before we indicate how to deduce this from our proof of Theorem 4, we first note the following results:

Proposition 2. *If A and B are two sets of distinct real numbers then $\#\{|a - b| : a \in A, b \in B\} \geq \min\{|A|, |B|\}$. If equality holds then either*

- *$A = B$ is an arithmetic progression; or*
- *$B = \{a + (2i + 1)d : 1 \leq 2i + 1 \leq 2N - 1\}$ with $A_0 = \{a + 2id : 0 \leq 2i \leq 2N\}$, and then A is either A_0, or A_0 less any one element; or*
- *$A = \{m - a, m + a\}$ and $B = \{m - b, m + b\}$ for some $a > b > 0$.*

The inequality in Proposition 2 can be proved by taking c to be the smallest number from either set (say from B), and then by noting that the numbers $a - c, a \in A$, are distinct, positive real numbers. That the enumerated cases are the only ones in which equality holds may be proved by induction on $\min\{|A|,|B|\}$, using the induction hypothesis on the smaller sets created by removing the largest number from each of A and B.

Proposition 3. *Suppose that $I \in \mathbb{I}_k$ and that $f : I \to \mathbb{R}$ is a map for which $|f(\mathbf{i}) - f(\mathbf{j})|$ is a function of $d(\mathbf{i},\mathbf{j})$ only. Then there exist constants α and β such that, for every $\mathbf{i} \in I$, either $f(\mathbf{i}) = \alpha + \beta i_j$ for some fixed j, or $f(\mathbf{i}) = \alpha$ or β depending on whether or not $\mathbf{i} \in T$, where T is a subgroup of S of index 2.*

Proposition 3 is easily proved by induction on k.

Sketch of the proof of proposition 1. If $|A| = 1$ then clearly $|D(A)| = 1$. If $n = 1$ then A is an arithmetic progression, by Proposition 2. We now proceed with the same induction as in the proof of Theorem 4, and then by induction on $h(= h(A))$, the maximum of $|A_{\mathbf{b}}|, \mathbf{b} \in B$. For $h = 1$, we know that B has the structure stated in Proposition 1 by induction, since $|D(B)| = |B|$ as in the proof of Theorem 4. Define $f(\mathbf{i}) = a_{\mathbf{b}}$ where $\mathbf{b} = \mathbf{a} + \sum_{j=1}^{k} i_j \mathbf{v}_j$. The result follows from Proposition 3.

Now suppose $h > 1$ and write $A^{(1)} = A$. By the proof of Theorem 4 we know that $|D(B^{(1)})| = |B^{(1)}|$ and $|D(A^{(2)})| = |A^{(2)}|$ where $B^{(1)} = B$ and $A^{(2)} = C$. We now apply the proof of Theorem 4 to $A^{(2)}$ and then to $A^{(3)}$, etc., to find a sequence of sets $A^{(1)} \supsetneq A^{(2)} \supsetneq \cdots \supsetneq A^{(h)}$ with each $h(A^{(j)}) = h + 1 - j$ and $|D(A^{(j)})| = |A^{(j)}|$. Note that $B^{(j)} = \{\mathbf{b} \in B : |A_{\mathbf{b}}| \geq j\}$.

We first prove Proposition 1 for $A^* := \{(\mathbf{b}, x) : \mathbf{b} \in B^{(h)}, x \in A_{\mathbf{b}}\}$. From the proof of Theorem 4 (taking $D = 0$) we see that there are no more than h elements in the union of all sets $\{|a - a'| : a, a' \in A_{\mathbf{b}}\}$. If $|A_{\mathbf{b}}| = h$ then, by Proposition 2, $A_{\mathbf{b}}$ must be an arithmetic progression; and the arithmetic progressions for any two such sets must have the same common difference. Moreover if $|A_{\mathbf{b}}| = |A_{\mathbf{b}'}| = h$ then $\#\{|a - a'| : a \in A_{\mathbf{b}}, a' \in A_{\mathbf{b}'}\} \leq h$ by the proof of Theorem 4, and so either $A_{\mathbf{b}} = A_{\mathbf{b}'}$ or they are two disjoint, but interwoven, arithmetic progressions, by Proposition 2. Thus the sets $A_{\mathbf{b}}$ of size h are either all identical (in which case A^* satisfies Proposition 1 by the induction hypothesis), or there are two possible such sets $A_{\mathbf{b}}$. In this case we may write each $\mathbf{b} = \mathbf{a} + \sum_{j=1}^{k} i_j \mathbf{v}_j$ by the induction hypothesis, and let $f(\mathbf{i})$ be the smallest element in $A_{\mathbf{b}}$. By Proposition 3 we deduce that Proposition 1 holds for A^*.

The result thus holds when $A^* = A$, that is, when there are h elements in every $A_{\mathbf{b}}$, or equivalently when $B^{(1)} = B^{(h)}$. If not then there exists $\mathbf{b} \in B^{(j)} \setminus B^{(j+1)}$ for some $j, 1 \leq j \leq h - 1$. Let $\mathbf{b}'$ be any point in $B^{(j+1)}$ and $D := d(\mathbf{b}', \mathbf{b})$. The induction hypothesis ensures that each $B^{(i)}$ is a lattice as described in the hypothesis of Proposition 1, and this particular lattice structure implies that there do not exist $\beta, \beta' \in B^{(j+1)}$ with $d(\beta, \beta') = D$. Therefore $\#\{|a - a'| : a \in A_{\mathbf{b}}, a' \in A_{\mathbf{b}'}\} = |A_{\mathbf{b}}|$, by the proof of Theorem 4. Using Proposition 2 we deduce that $A_{\mathbf{b}}$ and $A_{\mathbf{b}'}$ are interwoven disjoint arithmetic progressions, whose union is also an arithmetic progression. Thus $h(A_{\mathbf{b}'}) = j + 1$, so taking $\mathbf{b}' \in B^{(h)}$ we see that $j = h - 1$, and moreover all such sets $A_{\mathbf{b}'}$, $\mathbf{b}' \in B^{(h)}$ must be the identical arithmetic progression. But the same argument applies to every $\mathbf{b} \in B^{(h-1)}$, and so each such $A_{\mathbf{b}}$ is the same arithmetic progression interwoven between the elements in each $A_{\mathbf{b}'}$ with $\mathbf{b}' \in B^{(h)}$. Thus Proposition 1 holds for A.

4. FURTHER QUESTIONS. Proposition 2 inspires, and provides the answer in one dimension to, the following open problem: If A and B are finite sets of distinct vectors in $\mathbb{R}^n$ then show that the order of the set $D(A, B) = \{d(\mathbf{a}, \mathbf{b}) : \mathbf{a} \in A, \mathbf{b} \in B\}$ is at least $\min\{|A|, |B|\}$. This translates to finding a lower bound for the order of $\{ab/\gcd(a, b)^2 : a \in A, b \in B\}$ where A and B are sets of distinct positive integers.

Probably even more difficult would be to find a good lower bound for the order of $\{a/\gcd(a, b), b/\gcd(a, b) : a \in A, b \in B\}$. Generalizing Graham's Conjecture, we conjecture that the largest element of this set is $\geq \min\{|A|, |B|\}$ (the authors of **[3]** have informed us that they retract the claim at the end of the introduction to [3], which would have implied this conjecture).

ACKNOWLEDGMENT. We thank Seva Lev and Carl Pomerance for their helpful comments, and Sudakov for communicating his proof of Theorem 1.

REFERENCES

1. N. Alon, M. Nathanson, and I. Ruzsa, Adding distinct congruence classes modulo a prime, *J. Number Theory* **102** (1995) 250–255.
2. Y. Bilu, Addition of sets of integers of positive density, *J. Number Theory* **64** (1997) 233–275.
3. R. Balasubramanian and K. Soundararajan, On a conjecture of R. L. Graham, *Acta Arith.* **75** (1996) 1–38.
4. P. Erdős, On sets of distances of n points, *Amer. Math. Monthly* **53** (1946) 248–250.
5. G. Freiman, Foundations of a structural theory of set addition, *Transl. Math. Monographs* **37** (1973).
6. V. Lev, Structure theorem for multiple addition and the Frobenius problem, *J. Number Theory* **58** (1996) 79–88.
7. I. Z. Ruzsa, Sets of sums and differences, *Sém. Théorie Nombres Paris* (1984) 267–273.
8. I. Z. Ruzsa, On the number of sums and differences, *Acta Math. Hung* **59** (1992) 439–447.
9. I. Z. Ruzsa, Generalized arithmetical progressions and sumsets, *Acta Math. Hungar.* **65** (1994) 379–388.
10. M. Szegedy, The solution of Graham's greatest common divisor problem, *Combinatorica* **6** (1986) 67–71.
11. L. A. Székely, Crossing numbers and hard Erdős problems in discrete geometry, *Combin. Probab. Comput.* **6** (1997) 353–358.
12. A. Zaharescu, On a conjecture of Graham, *J. Number Theory* **27** (1987) 33–40.
13. W. T. Gowers, A new proof of Szemerédi's theorem for arithmetic progressions of length four, *Geom. Funct. Anal.* **8** (1998) 529–551.

ANDREW GRANVILLE is the Barrow Professor of Mathematics at the University of Georgia. He is a regular contributor to the MONTHLY, and was a recipient of the MAA's Hasse prize in 1995. His main research is in number theory and related topics.
University of Georgia, Athens, Georgia 30602-7403
andrew@math.uga.edu

FRIEDRICH ROESLER Harvard class of '68, was born in Saxony at the end of the second world war. He studied in Münster (Germany), Cambridge, and London and received his Ph.D. from the University of Münster. Since 1983 he has been a professor of mathematics at the Technical University of Munich. His current research interests lie in number theory and algebra,
Zentrum Mathematik der Technischen Universität München, Arcisstrasse 21, 80290 München, Germany
roesler@mathematik.tu-muenchen.de

Six Ways of Looking at Burtin's Lemma

S. Anoulova, J. Bennies, J. Lenhard, D. Metzler, Y. Sung, and A. Weber

In an article in this MONTHLY in 1953 Metropolis and Ulam asked for the expected number of components of the graph induced by a purely random mapping of a set of n points into itself [7]. This problem was solved one year later by L. Kruskal [6]. In 1955, L. Kac [4] computed the probability that this random graph is connected, that is, that the number of components is 1. In 1981, S. Ross [9] treated the same questions for more general random mappings in which the function values are independent and identically distributed but not necessarily uniform. The fundamental lemma of [9] had been proved earlier by the young Russian mathematician Y. D. Burtin, several months before his death in 1977 [2, Prop. 1]:

Burtin's lemma: Let $F(1), \dots, F(n)$ be independent and identically distributed with $P\{F(i) = j\} = p_j$, $j = 0, \dots, n$. Generate a random directed graph Γ with vertices $\{0, \dots, n\}$ by drawing an edge from i to $F(i)$ for each $i = 1, \dots, n$. Then this graph is connected with probability p_0.

The proofs of Burtin's lemma given in [2] and [9] both use induction on n, lumping together all those vertices directly connected to 0. In 1984, still another inductive proof was given by Jaworski [3]. The six ways of looking at Burtin's lemma presented here arose from the attempt of each of us to understand it better.

Burtin's lemma has interesting connections with the random generation of spanning trees. Assign to each pair (i, j) $(1 \le i \le n,\ 0 \le j \le n)$ the weight p_j, and consider the problem of generating a random spanning tree on $\{0, \dots, n\}$ with root 0 such that the probability of a tree is proportional to the product of all its edge weights. Propp and Wilson [8] describe how to do this in a straightforward way: Start at an arbitrary element i of $\{1, \dots, n\}$, and consider the iterates $F(i), F^2(i), \dots$ until the first time they hit 0. Delete the cycles of the path from i to 0 and take this as the trunk of the tree. Then take an element j not on the trunk (if there are any), proceed in the way described until you hit the trunk, delete the cycles, and so on. Burtin's lemma then tells us that the probability of never producing a cycle in all these attempts is just p_0. In fact, our Proof 4 computes this probability directly. Proof 5 provides a more economical algorithm for generating a random spanning tree with the desired distribution.

Propp and Wilson [8] also treat the more general scenario in which the weights of an edge (i, j) can be of the form p_{ij} rather than p_j only. They also relate the problem of generation of random spanning trees to that of exact simulation of the equilibrium of a Markov chain by their algorithm of "coupling from the past." In [8, Sec. 1.3], they give a short history of random spanning tree generation, including references both to the algebraic method (which relies on variants of the so called matrix tree theorem [1, Ch. 2, Thm. 8] and the method using Markov chains.

And now to the proofs. Let A (for "acyclic") be the event that Γ contains no cycle. One easily sees that A can also be described as the event that

1) Γ is a (directed) tree; or
2) Γ is connected (as an undirected graph); or
3) there is a directed path from each vertex $i = 1, \dots n$ to 0. We then say "Each $i = 1, \dots n$ chooses, directly or indirectly, the vertex 0."

The first proof is a direct computation of $\Pr(A)$.

Proof 1: We enumerate all graphs from each of whose vertices $1, \dots, n$ all choose, directly or indirectly, the vertex 0. Let m_i be the number of immediate predecessors of the vertex i. Obviously $m_0 \geq 1$ and $\Sigma_{i=0}^{n} m_i = n$.

Construction:

a) Given $\{m_i\}$, choose successively for each vertex $i = 1, \dots, n$ its m_i immediate predecessors. For $i = 1$ there are $\binom{n-1}{m_1}$ possibilities; $F(1) = 1$ is not allowed since this would create a cycle. For $i = 2$ there are two cases:
   (i) If $F(2) = 1$, then $F(1) = 2$ is not allowed and there are $\binom{n - m_1 - 1}{m_2}$ possibilities.
   (ii) If $F(2) \neq 1$, then $F(2) = 2$ is not allowed and there are also $\binom{n - m_1 - 1}{m_2}$ possibilities.

   This argument holds for all k so in general there are $\binom{n - m_1 - \cdots - m_{k-1} - 1}{m_k}$ possibilities to choose the m_k immediate predecessors of vertex k.
b) The m_0 vertices that are left are the immediate predecessors of the vertex 0.

In all there are

$$\binom{n-1}{m_1}\binom{n-m_1-1}{m_2}\cdots\binom{n-m_1-\cdots-m_{n-1}-1}{m_n}$$
$$= \binom{n-1}{m_0 - 1, m_1, \dots, m_n}$$

possibilities to construct such a graph for given $m_0, \dots, m_n$.

Summing over all m_i we get

$$\Pr(A) = \sum_{\substack{m_0 \geq 1, \\ \Sigma m_i = n}} \binom{n-1}{m_0 - 1, m_1, \dots, m_n} p_0^{m_0} \cdots p_n^{m_n}$$
$$= p_0 (p_0 + \cdots + p_n)^{n-1} = p_0. \qquad \blacksquare$$

Proof 2 is inductive and works by lumping together an individual n and the one it chooses.

Proof 2: Suppose the proposition is proved for $n - 1 \geq 2$ individuals; for $n = 2$ (exactly one voter) it is trivial. We partition A according to the choice of individual n.

If $F(n) = 0$, we combine the individuals 0 and n into one new individual and start again with $n - 1$ individuals. By the induction hypothesis the contribution of this case to $\Pr(A)$ is $p_0(p_0 + p_n)$.

If $F(n) = j$, $j \in \{1, \ldots, n - 1\}$, we combine individuals j and n and obtain probability weights $p_0, p_1, \ldots, p_j + p_n, \ldots, p_{n-1}$; hence this case contributes the probability $p_j p_0$.

Finally, if $F(n) = n$, we have a cycle, so this case contributes nothing.

Summing over all these possibilities we get:

$$\Pr(A) = p_0(p_0 + p_n) + \left(\sum_{j=1}^{n-1} p_j\right) \cdot p_0 = p_0\left(\sum_{j=0}^{n} p_j\right) = p_0. \qquad \blacksquare$$

The next proof is also by induction, but in this case we show that lumping together individuals $n - 1$ and n does not change $\Pr(A)$. Iterating this argument then proves the proposition.

Proof 3: We imagine that only the individuals $1, \ldots, n - 2$ have already chosen their successors.

We consider two scenarios:

(i) with individuals $n - 1$ and n left to make their choice,
(ii) with the composite individual $(n - 1)'$, which is obtained by lumping together individuals $n - 1$ and n. This individual has weight $p_{(n-1)'} = p_{n-1} + p_n$.

Obviously the probability that there is no cycle so far is the same in both scenarios.

Let T_k be the set of all individuals who have, directly or indirectly, chosen k. At this moment, in (i), T_0, T_{n-1}, and T_n are disjoint and are trees since Γ so far contains no cycles. In (ii) the same holds for T_0 and $T_{(n-1)'}$.

In scenario (i) a cycle in Γ would be created if $F(n - 1) \in T_{n-1}$ or $F(n) \in T_n$ or $\{F(n - 1) \in T_n$ and $F(n) \in T_{n-1}\}$. The probability for this is $S_{n-1} + S_n$, where S_{n-1} and S_n designate the sums of the weights of all vertices (including the root) in T_{n-1} and T_n, respectively.

In scenario (ii) the choice of $(n - 1)'$ produces a cycle if and only if $F((n - 1)') \in T_{(n-1)'}$. The probability of this is $S_{(n-1)'} = S_n + S_{n-1}$. $\blacksquare$

In Proof 4 we consider the stochastic process of the successive choices of the individuals.

Proof 4: Let the n individuals make their choices in succession beginning with individual n and ending with individual 1. Let C_k be the event that individual k completes the first cycle. We claim:

$$\Pr(C_k) = \frac{p_k}{\sum_{i=0}^{k} p_i}.$$

If this claim holds, the proposition follows by an easy calculation:

$$\Pr(A) = \Pr\left(\bigcap_{k=n}^{1} C_k^c\right) = \prod_{k=n}^{1}\left(1 - \frac{p_k}{\sum_{i=0}^{k} p_i}\right)$$

$$= \frac{\sum_{i=0}^{n-1} p_i}{\sum_{i=0}^{n} p_i} \cdot \frac{\sum_{i=0}^{n-2} p_i}{\sum_{i=0}^{n-1} p_i} \cdot \cdots \cdot \frac{p_0}{p_0 + p_1} = p_0.$$

We check the correctness of the claim. Suppose that the individuals $\{n, \dots, k+1\}$ have not completed a cycle: this is the case if and only if each of them has chosen (perhaps indirectly) one of $\{0, \dots, k\}$, otherwise a directed path along the arrows would start from this individual without reaching any element of $\{0, \dots, k\}$, and would therefore be a cycle. For example, in Figure 1, n chooses $(n-2), (n-1)$ chooses k, and $(n-2)$ chooses k (indirectly).

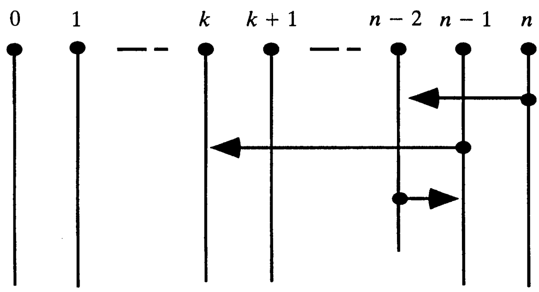


Figure 1

The event that individual k now completes the first cycle consists of two parts:

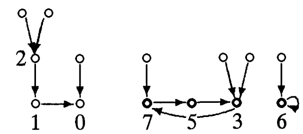
(i) $F(k) = k$, which happens with probability p_k.
(ii) $F(k) \in \{k+1, \dots, n\}$, and $F(k)$ has chosen (perhaps indirectly) k; the first of these occurrences happens with probability $\sum_{i=k+1}^{n} p_i$. As to the second occurrence, consider the path starting at $F(k)$. The probability that it hits the set $\{0, \dots, k\}$ in k is $p_k / \sum_{i=0}^{k} p_i$. Therefore:

$$\Pr(C_k) = p_k + \sum_{i=k+1}^{n} p_i \left(\frac{p_k}{\sum_{j=0}^{k} p_j}\right) = \frac{p_k}{\sum_{i=0}^{k} p_i}. \qquad \blacksquare$$

Proof 5 gives a bijection between cycle-free graphs of F and graphs where $F(1) = 0$. It also provides an economical algorithm for generating a random spanning tree with root 0.

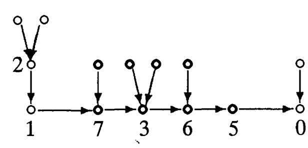
Proof 5: Consider the set B of all graphs Γ where $1 \to 0$ is an edge. B occurs with probability p_0. We want to prove $\Pr(A) = \Pr(B)$. We do this by constructing a bijective map $f: B \to A$ with the property $\Pr(f(b)) = \Pr(b)$ for all $b \in B$.

Consider a graph $b \in B$. For example:



The graph defines a partition into cycles of all the vertices that lie on a cycle. In our example: (753)(6).

Now we define $f(b) \in A$ by assigning the following graph to the corresponding permutation $(753)(6) = \binom{3567}{7365}$:



Both graphs occur with the same probability, namely $p_0^2 p_1 p_2^2 p_3^3 p_5 p_6^2 p_7^2$, because we do not change the number of edges that point toward each vertex.

The example describes how to construct a measure-preserving bijection (each permutation has a unique cycle–representation) for each selection of vertices that builds the cycles or the path between 1 and 0. Together the bijections define the desired f. ∎

Proof 6 uses the fact that a cycle-free F codes a tree with root 0, and also gives a simple algorithm to generate a random spanning tree in a special case.

Proof 6: The connected graph without cycles generated by F (when A occurs) can also be considered as a labeled rooted tree. In this context it is more natural to think of $F(i)$ as the predecessor rather than the successor of i. Each vertex i has exactly one predecessor $F(i)$. The root is zero.

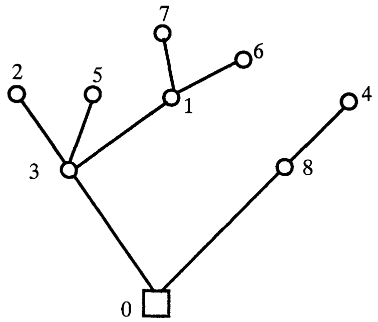
According to Knuth [**5**, p. 389] we can code each rooted $\{0,\dots,n\}$–labeled tree f by a vector $K(f) = (K_1(f),\dots,K_n(f)) \in \{0,\dots,n\}^n$, see Fig. 2.

The following proof is based on the equation

$$\Pr(A) = \sum_{x \in \{0,\dots,n\}^n} \Pr\big(F = K^{-1}(x)\big)$$

and the simple structure of the summation range. Three properties of K are important for the computation of $\Pr(F = K^{-1}(x))$:

(i) $K_n(f)$ is the label of the root of f.
(ii) The number of children of a node equals the number of occurrences of its label in the multiset $[K_1(f),\dots,K_n(f)]$.
(iii) Every $x \in \{0,\dots,n\}^n$ codes a tree.



$f(7)$	$f(6)$	$f(5)$	$f(4)$	$f(8)$	$f(2)$	$f(1)$	$f(3)$
1	1	3	8	0	3	3	0
$K_1(f)$	$K_2(f)$	$K_3(f)$	$K_4(f)$	$K_5(f)$	$K_6(f)$	$K_7(f)$	$K_8(f)$

Figure 2. Knuth's coding of a rooted $\{0,\ldots,n\}$-labeled tree f into $K(f) \in \{0,\ldots,n\}^n$: We get the list of numbers $K_1(f),\ldots,K_n(f)$ by iteratively removing the highest labeled leaf and noting the label of its predecessor. In each iteration step, a node is considered to be leaf, if all its children are already removed.

From (i) follows that $\Pr(F = K^{-1}(x)) = 0$ for $K_n(f) \neq 0$, because if F is a tree at all, it has 0 as root. For every rooted labeled tree f, (ii) implies equality of the multisets $[f(1),\ldots,f(n)]$ and $[K_1(f),\ldots,K_n(f)]$. Let T be the set of all $\{0,\ldots,n\}$-labeled trees with root 0. We obtain:

$$\sum_{f\in T} \Pr(F = f) = \sum_{f\in T} p_{f(1)} \cdots p_{f(n)} = \sum_{f\in T} p_{K_1(f)} \cdots p_{K_n(f)}$$

$$= \sum_{x\in\{0,\ldots,n\}^{n-1}\times\{0\}} p_{x_1} \cdots p_{x_n} = (p_0 + \cdots + p_n)^{n-1} \cdot p_0 = p_0.$$

Note that this also gives an algorithm for generating a random spanning tree: Just take $K^{-1}(X_1,\ldots,X_n)$ with $X_1,\ldots,X_n$ independent and identically distributed according to the weights of the random mapping F.

The tree can be recovered from the sequence by successively assigning to the $K_i(f)$'s their successors $K_i'(f)$. Remembering the rule of construction of the $K_i(f)$'s, one gets the arrangement illustrated in Figure 3.

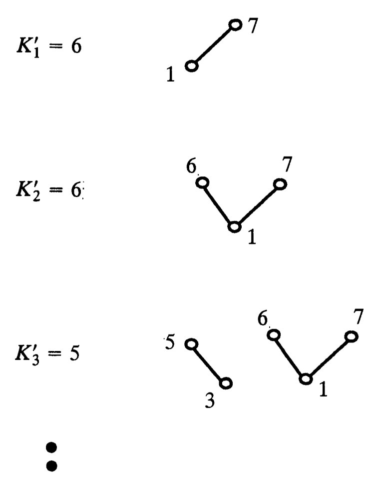


Figure 3

Formally

$$K_i' = \max\{\{1,\ldots,n\} \setminus \{K_1',\ldots,K_{i-1}',K_i,\ldots,K_n\}\}, \quad 1 \le i \le n,$$

in our example: $K_1', K_2', K_3', \ldots, K_8' = 7, 6, 5, 4, 8, 2, 1, 3.$ ■

ACKNOWLEDGMENTS. We thank Anton Wakolbinger and Brooks Ferebee for comments that have greatfully improved the presentation.

REFERENCES

1. B. Bollobas, *Graph Theory: An Introductory Course*, Springer Verlag (1979), Graduate Texts in Mathematics 63.
2. Y. D. Burtin, On a Simple Formula for Random Mappings and its Applications, *J. Appl. Prob.* **17** (1980) 403–414.
3. J. Jaworski, On a Random Mapping (T, p_j), *J. Appl. Prob.* **21** (1984), 186–191.
4. L. Kac, Probability of Indecomposability of a Random Mapping Function, *Ann. Math. Statist.* **26** (1955) 512–517.
5. D. E. Knuth, *The Art of Computer Programming*, Vol.1 (1968), Addison Wesley.
6. M. D. Kruskal, The Expected Number of Components Under a Random Mapping Function, *Amer. Math. Monthly* **61** (1954) 392–397.
7. N. Metropolis and S. Ulam, A Property of Randomness of an Arithmetical Function, *Amer. Math. Monthly* **60** (1953) 252–253.
8. J. G. Propp and D. B. Wilson, How to Get a Perfectly Random Sample from a Generic Markov Chain and Generate a Random Spanning Tree of a Directed Graph, preprint (1998), http://dimacs.rutgers.edu/~ dbwilson/exact.html/
9. S. M. Ross, A Random Graph, *J. Appl. Prob.* 18 (1981), 309–315

SVETLANA ANOULOVA received her Ph.D. in 1979 at the University of Moscow. She is working on limit theorems for stochastic processes at the Institute for Control Sciences of the Russian Academy of Sciences.

JÜRGEN BENNIES is a Ph.D. student in mathematics in Frankfurt, Germany. The subjects of his research are random walks, trees, and mappings.
bennies@math.uni-frankfurt.de

JOHANNES LENHARD received his Ph.D. in mathematics from the University of Frankfurt, Germany, in 1998. In his thesis he examined a way of looking at a mathematical problem of population biology.
Lenhard@mathematik.uni-frankfurt.de

DIRK METZLER is a student of mathematics at the Johann Wolfgang Goethe-Universitat in Frankfurt, Germany. He is just about to finish his Ph.D. thesis on Poisson approximations for pattern configurations on related DNA-strands.
dmetzler@math.uni-frankfurt.de

YÜ SUNG received her Ph.D. from Frankfurt University. Her main research interests are in probability theory and finance.
y.sung@mathematik.uni-frankfurt.de

ANDREAS WEBER is an undergraduate student of mathematics at Frankfurt University (Germany).
And_Weber@compuserve.com

Johann Wofgang Goethe-Universität, Fachbereich Mathematik, AG Stochastik, Robert–Mayer–Str.10, D–60054 Frankfurt, Germany

NOTES

Edited by **Jimmie D. Lawson and William Adkins**

Lexell's Theorem Via an Inscribed Angle Theorem

Hiroshi Maehara

We present a simple inscribed angle theorem in spherical geometry, and apply it to give a short proof of Lexell's theorem.

Theorem 1. *For any spherical triangle ABC inscribed in a fixed circular arc Γ with end-points A, B, the value of $\angle C - (\angle A + \angle B)$ is constant.*

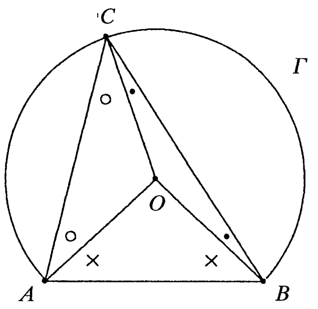


Figure 1

Proof: Let O be the center of the spherical cap determined by Γ. Then, since the base angles of a spherical isosceles triangle are equal, it follows easily from Figure 1 that

$$\angle C - (\angle A + \angle B) = \pm 2\angle OAB,$$

where the sign is $+$ if Γ is a minor arc, and $-$ otherwise. ■

Let $|ABC|$ denote the area of a spherical triangle ABC on the unit sphere. Then by Girard's formula, we have $|ABC| = \angle A + \angle B + \angle C - \pi$.

Theorem 2 (Lexell). *Let ABC be a spherical triangle on the unit sphere, and let $\mathscr{H}$ be the hemisphere bounded by the great circle AB and containing C. Then the locus of the point $X \in \mathscr{H}$ satisfying $|ABX| = |ABC|$ is the circular arc A^*CB^*, where A^*, B^* are the antipodal points of A, B, respectively.*

Proof: It suffices to show that $|ABX| = |ABC|$ for any point X on the circular arc A^*CB^* $(X \neq A^*, X \neq B^*)$, By theorem 1, we have $\angle A^*CB^* - (\angle CA^*B^* + \angle CB^*A^*) = \angle A^*XB^* - (\angle XA^*B^* + \angle XB^*A^*)$. Since $\angle A^*XB^* = \angle AXB$,

$\angle XA^*B^* = \pi - \angle XAB$, $\angle XB^*A^* = \pi - \angle XBA$, we have $\angle AXB + \angle BAX + \angle ABX = \angle ACB + \angle BAC + \angle ABC$. Hence, by Girard's formula, we have $|ABX| = |ABC|$. ■

For a different proof of Lexell's theorem, see L. Fejes Tóth, *Lagerungen in der Ebene auf der Kugel und im Raum*, Springer-Verlag, Berlin, 1972, p. 23.

College of Education, Ryukyu University, Nishihara, Okinawa, 903-0213 Japan.
hmaehara@edu.u-ryukyu.ac.jp

A Characteristic Property of Differentiation

Khristo Boyadzhiev

We offer here a simple exercise in calculus with a flavor of functional analysis. The differentiation operator $D: f \to f'$ is a fundamental operator in calculus and it is interesting to consider what properties distinguish it from all other operators on functions. One important theorem says that if a differentiable function $f(x)$ has a relative minimum (or maximum) at $x = a$, then $f'(a) = 0$. As we shall see now, this property "almost" characterizes D.

Notation. For convenience we consider only polynomials. Let P be the set of all polynomials and let p_n, $n = 0, 1, \ldots,$ be the basic polynomials:

$$p_0(x) = 1, p_1(x) = x, \ldots, p_n(x) = x^n, \ldots .$$

When $\delta : P \to P$ is a linear operator, we denote its action on $p \in P$ by $\delta[p]$. Thus $\delta[p]$ is again a polynomial and its value at some number x is written as $\delta[p](x)$.

Theorem 1. *Let $\delta : P \to P$ be a linear operator. Then the following are equivalent:*

(i) *If p has a relative minimum at $x = a$, then $\delta[p](a) = 0$.*
(ii) $\delta = \delta[p_1]D$.

In particular, if $\delta[p_1] = p_0$, then $\delta = D$. (Here "minimum" can be replaced by maximum.")

Proof: The implication (ii) $\to$ (i) is immediate, so we focus on (i) $\to$ (ii). First we want to show that every linear operator on P has a convenient general form. By Taylor's formula, for any polynomial p and any number a:

$$p(x) = \sum_{k=0}^{\infty} \frac{p^{(k)}(a)}{k!}(x-a)^k.$$

The sum is finite and we write "∞" just for convenience. Applying δ to both sides (as polynomials of x, with a fixed) we obtain

$$\delta[p] = \sum_{k=0}^{\infty} \frac{p^{(k)}(a)}{k!}\delta\left[(x-a)^k\right] \tag{1}$$

where $\delta[(x-a)^k]$ are polynomials of x. Setting

$$g_k(a) = \frac{1}{k!}\delta\left[(x-a)^k\right](a), \tag{2}$$

i.e., evaluating these polynomials at $x = a$, we define new polynomials g_k, $k = 0, 1, \dots$.

It is clear that (2) defines functions of the variable a, but why are these functions polynomials? Good question! To answer it we use the binomial formula for $(x-a)^k$ and the linearity of δ. Now (1) can be written in the form

$$\delta[p](a) = \sum_{k=0}^{\infty} g_k(a)p^{(k)}(a)$$

or simply

$$\delta[p] = g_0 + g_1 p' + g_2 p'' + \cdots . \tag{3}$$

This is the representation we need: the action of δ is expressed in a simple way in terms of the polynomials g_k. Notice that we did not use here property (i). Therefore, the general representation (3) is true for every linear operator on the polynomials.

It turns out that under condition (i) we have $g_k = 0$ for every $k > 1$. Indeed, consider the polynomial

$$f(x) = \frac{1}{2}(x-a)^2 + \frac{\lambda}{k!}(x-a)^k$$

which is specially designed to serve our purpose. Here a and λ are arbitrary real numbers and the integer $k > 2$. We have $f'(a) = 0$, $f''(a) = 1$, so f has a relative minimum at $x = a$. According to property (i)

$$\delta[f](a) = g_2(a) + \lambda g_k(a) = 0$$

Since this is true for all λ and a, we conclude that $g_k = 0$ identically for all $k > 1$. Also, $g_0 = \delta[p_0] = 0$, as p_0 has minimum at each number. Finally, using the linearity of δ we obtain

$$\begin{aligned} g_1(a) &= \delta[(x-a)](a) = \delta[p_1 - ap_0](a) \\ &= \delta[p_1](a) - a\delta[p_0](a) = \delta[p_1](a). \end{aligned}$$

Therefore, the representation (3) turns into

$$\delta[p] = \delta[p_1]p'$$

for every polynomial p. ■

The same proof gives the following.

Theorem 2. *Let $\delta : P \to P$ be a linear operator with the following property (Minimum Principle): $\delta[p](a) \ge 0$ whenever a polynomial p has a relative minimum at some number $x = a$. Then $\delta[p] = g_1 p' + g_2 p''$ for all $p \in P$, where the polynomials g_1, g_2 are defined in* (2) *and $g_2 \ge 0$.*

Theorem 2 naturally extends to polynomials of many variables: any linear operator $\delta : P \to P$ satisfying the Minimum Principle is a second-order elliptic partial differential operator. For instance, Markov processes (semigroups) in diffusion theory have generators that satisfy the Minimum Principle [1]. There-

fore, we conclude that diffusion in nature is governed by second-order elliptic partial differential operators. Theorem 2 (in a different form) originates from A. Kolmogorov. Some others contributed to it, providing modifications and extensions: comments and references can be found in [**1**, Chapter 5] and [**2**, Chapter XIII].

REFERENCES

1. E. B. Dynkin, *Markov Processes*, vol 1., Springer-Verlag, Berlin, 1965.
2. K. Yosida, *Functional Analysis*, Springer-Verlag, New York, 1980.

Ohio Northern University, Ada, Ohio 45810.
k-boyadzhiev@onu.edu

A Weighted Mixed-Mean Inequality

Kiran S. Kedlaya

In [**4**], the author established the following inequality conjectured by Holland [**3**]. Unbeknownst to either of these parties, the same inequality had been earlier announced by Nanjundiah [**8**] without proof.

Theorem 1. *Let $x_1, x_2, \dots, x_n$ be positive real numbers. The arithmetic mean of the numbers*

$$x_1, \sqrt{x_1 x_2}, \dots, \sqrt[n]{x_1 x_2 \cdots x_n}$$

does not exceed the geometric mean of the numbers

$$x_1, \frac{x_1 + x_2}{2}, \dots, \frac{x_1 + x_2 + \cdots + x_n}{n}.$$

Equality holds if and only if $x_1 = x_2 = \cdots = x_n$.

Here we prove the following weighted extension of Theorem 1.

Theorem 2. *Let $x_1, \dots, x_n, w_1, \dots, w_n$ be positive real numbers, and define $s_i = w_1 + \cdots + w_i$ for $i = 1, \dots, n$. Assume that*

$$\frac{w_1}{s_1} \geq \frac{w_2}{s_2} \geq \cdots \geq \frac{w_n}{s_n}. \tag{1}$$

Then the weighted arithmetic mean of the numbers

$$x_1, x_1^{w_1/s_2} x_2^{w_2/s_2}, \dots, x_1^{w_1/s_n} x_2^{w_2/s_n} \cdots x_n^{w_n/s_n}$$

does not exceed the weighted geometric mean of the numbers

$$x_1, \frac{w_1}{s_2} x_1 + \frac{w_2}{s_2} x_2, \dots, \frac{w_1}{s_n} x_1 + \frac{w_2}{s_n} x_2 + \cdots + \frac{w_n}{s_n} x_n$$

when each mean is taken with weights $w_1/s_n, w_2/s_n, \dots, w_n/s_n$. In other words,

$$\prod_{i=1}^{n} \left(\sum_{j=1}^{i} \frac{w_j}{s_i} x_j \right)^{w_i/s_n} \geq \sum_{j=1}^{n} \frac{w_j}{s_n} \prod_{i=1}^{j} x_i^{w_i/s_j}. \tag{2}$$

Equality holds if and only if $x_1 = \cdots = x_n$.

The constraint (1) might not be the weakest possible, but some constraint is definitely necessary; for example, one needs to have

$$\left(\frac{w_1}{s_1}\right)^{w_1}\left(\frac{w_2}{s_2}\right)^{w_2}\cdots\left(\frac{w_{n-1}}{s_{n-1}}\right)^{w_{n-1}} \geq \left(\frac{w_n}{s_n}\right)^{s_{n-1}}$$

or else (2) fails for $x_n \gg x_{n-1} \gg \cdots \gg x_1$. Preliminary calculations suggest that this condition might even be sufficient, but a proof seems difficult. Theorem 2 is asserted without any condition on the weights in [**1**, pp. 122–123]; of course the proof given there is incorrect.

The ingredients of the proof of Theorem 2 are the same as in [**4**], except that we use induction to simplify the computations; one may unravel the induction to obtain a proof that, in the case of equal weights, coincides with the proof in [**4**]. A different inductive proof of Theorem 1, using Lagrange multipliers, appears in [**5**].

Proof: We prove Theorem 2 by proving an analogue of Rado's inequality [**2**, Theorem 60] in this setting. Namely, if L_n and R_n denote the left and right sides of (2), we prove that

$$\left(\frac{L_n}{R_n}\right)^{s_n} \geq \left(\frac{L_{n-1}}{R_{n-1}}\right)^{s_{n-1}} \tag{3}$$

for $n > 1$. We note in passing that a similar argument gives an analogue of Popoviciu's inequality [**9**]:

$$s_n(L_n - R_n) \geq s_{n-1}(L_{n-1} - R_{n-1}).$$

Unraveling (3), we see that it is equivalent to

$$\left(\sum_{j=1}^{n}\frac{w_j}{s_n}x_j\right)^{w_n}\left(\sum_{j=1}^{n-1}\frac{w_j}{s_{n-1}}\prod_{i=1}^{j}x_i^{w_i/s_j}\right)^{s_{n-1}} \geq \left(\sum_{j=1}^{n}\frac{w_j}{s_n}x_j^{w_j/s_j}\prod_{i=1}^{j-1}x_i^{w_i/s_j}\right)^{s_n}. \tag{4}$$

We prove this inequality in two steps. First, we observe that

$$\sum_{j=1}^{n-1}\frac{w_j}{s_{n-1}}\prod_{i=1}^{j}x_i^{w_i/s_j} = \sum_{j=1}^{n}\left[\frac{w_js_n - w_ns_j}{s_{n-1}s_n}\prod_{i=1}^{j}x_i^{w_i/s_j} + \frac{s_{j-1}w_n}{s_{n-1}s_n}\prod_{i=1}^{j-1}x_i^{w_i/s_{j-1}}\right];$$

since $w_js_n \geq w_ns_j$ by (1), we may apply the weighted arithmetic-mean, geometric-mean inequality to each summand on the right side and obtain

$$\sum_{j=1}^{n-1}\frac{w_j}{s_{n-1}}\prod_{i=1}^{j}x_i^{w_i/s_j} \geq \sum_{j=1}^{n}\frac{w_j}{s_n}x_j^{\frac{w_js_n - w_ns_j}{s_js_{n-1}}}\prod_{i=1}^{j-1}x_i^{\frac{w_is_n}{s_js_{n-1}}}. \tag{5}$$

Second, we apply Hölder's inequality to get

$$\left(\sum_{j=1}^{n}\frac{w_j}{s_n}x_j^{\frac{w_js_n - w_ns_j}{s_js_{n-1}}}\prod_{i=1}^{j-1}x_i^{\frac{w_is_n}{s_js_{n-1}}}\right)^{s_{n-1}/s_n}\left(\sum_{j=1}^{n}\frac{w_j}{s_n}x_j\right)^{w_n/s_n} \geq \sum_{j=1}^{n}\frac{w_j}{s_n}x_j^{w_j/s_j}\prod_{i=1}^{j-1}x_i^{w_i/s_j}. \tag{6}$$

Together, (5) and (6) imply (4), and (2) now follows by induction on n (since equality vacuously holds for $n = 1$). The equality condition also follows by induction: if equality holds in (2), then equality in (3) forces $x_1 = \cdots = x_{n-1}$ by hypothesis, and equality in (6) forces $x_1 = x_n$.

We mention here three ways in which Theorem 2 can be extended easily. First, one can replace the arithmetic and geometric means by the r-th and s-th power means, respectively, for any $r > s$; the corresponding analogue of Theorem 1 is formulated in [**6**]. Recall that for $r \neq 0$, the r-th power mean of $x_1, \dots, x_n$ with weights $w_1, \dots, w_n$ is given by

$$\left(\frac{w_1}{s_n}x_1^r + \frac{w_2}{s_n}x_2^r + \cdots + \frac{w_n}{s_n}x_n^r\right)^{1/r}.$$

Extending by continuity to $r = 0$ yields the weighted geometric mean. The statement of the inequality then becomes

$$\left(\sum_{i=1}^{n}\frac{w_i}{s_n}\left(\sum_{j=1}^{i}\frac{w_j}{s_i}x_j^r\right)^{s/r}\right)^{1/s} \geq \left(\sum_{j=1}^{n}\frac{w_j}{s_n}\left(\sum_{i=1}^{j}\frac{w_i}{s_j}x_i^s\right)^{r/s}\right)^{1/r},$$

the Rado and Popoviciu-type inequalities become

$$s_n\left(L_n^k - R_n^k\right) \geq s_{n-1}\left(L_{n-1}^k - R_{n-1}^k\right) \quad k = r, s,$$

and the proofs carry over upon replacing the weighted arithmetic-mean, geometric-mean inequality by the weighted power mean inequality, and Hölder's inequality by Minkowski's inequality [**2**, Theorem 24]. This last inequality appears to hold for all $k \in [s, r]$, but I do not have a proof.

Second, one can prove a analogue of Theorem 2 for Hermitian matrices, using the arithmetic and harmonic means, following Mond and Pečarić [**7**], who proved such an analogue of Theorem 1 using a matricial Minkowski inequality.

Third, one may use a straightforward limiting argument to deduce the following continuous analogue of Theorem 2. We leave the formulation of the corresponding power mean generalization to the reader.

Theorem 3. *Let $f(x)$ and $w(x)$ be continuous positive-valued functions on $[0,1]$, and let $W(x) = \int_0^x w(t)\,dt$. Assume that $w(x)/W(x)$ is nondecreasing on $(0,1]$. Then*

$$\int_0^1 \exp\left(\frac{w(y)}{W(1)}\log\int_0^y \frac{w(x)}{W(y)}f(x)\,dx\right)dy \geq \int_0^1 \frac{w(y)}{W(1)}\exp\left(\int_0^y \frac{w(x)}{W(y)}\log f(x)\,dx\right)dy.$$

Finally, we use Theorem 2 to generalize a well-known inequality of Carleman: for a sequence $\{a_n\}_{n=1}^{\infty}$ of positive real numbers with $\Sigma a_n < \infty$,

$$\sum_{k=1}^{\infty}(a_1 \cdots a_k)^{1/k} < e\sum_{k=1}^{\infty}a_k.$$

It was observed in [**3**] and in [**8**] that this inequality follows from Theorem 1. We refine this observation slightly to obtain a weighted version of Carleman's inequality. Surprisingly (to the author, at least), the constant on the right side does not depend on the weights!

Theorem 4. *Let $w_1, w_2, \dots$ be a sequence of positive real numbers, and define $s_i = w_1 + \cdots + w_i$ for $i = 1, 2 \dots$. Assume that*

$$\frac{w_1}{s_1} \geq \frac{w_2}{s_2} \geq \cdots.$$

Then for any sequence $a_1, a_2, \dots$ of positive real numbers with $\Sigma_k w_k a_k < \infty$,

$$\sum_{k=1}^{\infty} w_k a_1^{w_1/s_k} \cdots a_k^{w_k/s_k} < e\sum_{k=1}^{\infty}w_k a_k.$$

Proof: Taking $x_k = a_k$ for $k = 1, \dots, n$ in Theorem 2, we obtain

$$\sum_{k=1}^{n} \frac{w_k}{s_n} a_1^{w_1/s_k} \cdots a_k^{w_k/s_k} \le \prod_{k=1}^{n} \left(\sum_{i=1}^{k} \frac{w_i}{s_i} a_i \right)^{w_k/s_n}.$$

Of course $\sum_{i=1}^{k} w_i a_i \le \sum_{i=1}^{n} w_i a_i$, and so

$$\sum_{k=1}^{n} w_k a_1^{w_1/s_k} \cdots a_k^{w_k/s_k} \le \frac{s_n}{s_1^{w_1/s_n} \cdots s_n^{w_n/s_n}} \sum_{k=1}^{n} a_k.$$

In addition, using partial summation and the bound $\log x < x - 1$ for $x > 0$, we get

$$\begin{aligned} \frac{s_n}{s_1^{w_1/s_n} \cdots s_n^{w_n/s_n}} &= \exp \sum_{k=1}^{n} \frac{w_k}{s_n} (\log s_n - \log s_k) \\ &= \exp \sum_{k=1}^{n-1} \frac{s_k}{s_n} (\log s_{k+1} - \log s_k) \\ &< \exp \sum_{k=1}^{n-1} \left(\frac{s_{k+1}}{s_n} - \frac{s_k}{s_n} \right) = \exp\left(1 - \frac{s_1}{s_n}\right) < e. \end{aligned}$$

Thus we have the desired inequality except with n in place of ∞, but taking $n \to \infty$ gives what we want. ■

Again, one can easily state and prove power mean and continuous analogues, and again the conditions on the weights are probably not the weakest possible.

ACKNOWLEDGMENTS. The author is supported by an NDSEG graduate fellowship. Thanks to Lenny Ng for commenting on an early draft of the manuscript.

REFERENCES

1. P. S. Bullen, D. S. Mitrinović, and P. M. Vasić (eds.), *Means and Their Inequalities*, Reidel, 1988.
2. G. Hardy, J. E. Littlewood, and G. Pólya, *Inequalities*, second edition, Cambridge University Press, Cambridge, 1951.
3. F. Holland, On a mixed arithmetic-mean, geometric-mean inequality, *Math. Competitions* **5** (1992) 60–64.
4. K. Kedlaya, Proof of a mixed arithmetic-mean, geometric-mean inequality, *Amer. Math. Monthly* **101** (1994) 355–357.
5. T. Matsuda, An inductive proof of a mixed arithmetic-geometric mean inequality, *Amer. Math. Monthly* **102** (1995) 634–637.
6. B. Mond and J. E. Pečarić, A mixed means inequality, *Austral. Math. Soc. Gaz.* **23** (1996) 67–70.
7. B. Mond and J. E. Pečarić, A mixed arithmetic-mean–harmonic-mean matrix inequality, *Lin. Algebra Appl.* **237 / 238** (1996) 449–454.
8. T. S. Nanjundiah, Sharpening of some classical inequalities, *Math. Student* **20** (1952) 24–25.
9. T. Popoviciu, Asupra mediilor aritmetice si medie geometrice (Romanian), *Gaz. Mat. Bucharest* **40** (1934) 155–160.

Massachusetts Institute of Technology, Cambridge, MA 02139
kedlaya@math.mit.edu

UNSOLVED PROBLEMS

Edited by **Richard Nowakowski**

In this department the MONTHLY presents easily stated unsolved problems dealing with notions ordinarily encountered in undergraduate mathematics. Each problem should be accompanied by relevant references (if any are known to the author) and by a brief description of known partial or related results. Typescripts should be sent to Richard Nowakowski, Department of Mathematics & Statistics & Computing Science, Dalhousie University, Halifax NS, Canada B3H 3J5, rjn@mscs.dal.ca

Periods in Taking and Splitting Games

Ian Caines, Carrie Gates, Richard K. Guy, and Richard J. Nowakowski

In 1997, J. H. Conway asked who wins *Couples-Are-Forever*? This game is played by two players playing alternately with heaps of counters. A move is to choose a heap and split it into two non-empty heaps, except that no heap of 2 may be split, hence the name. The player who moves last wins.

Without the exception, the game is easy to analyze. The next player wins if and only if there is an even number of heaps that contain an odd number of counters. This is the archetypal *she-loves-me-she-loves-me-not* game found in [**2**, pp. 113, 115].

Recall that the *nim-value* of a position G, denoted by $\mathscr{G}(G)$, is defined inductively. The end-positions, positions from which there are no moves, have value zero. Any other position has value the minimum excluded non-negative integer (*mex* for short) that does not occur among the values of its followers, i.e., those positions that can be reached in one move. If the nim-value of a position is zero then the next player cannot win; if it is non-zero then the next player does have a winning strategy.

Couples-are-Forever is a *disjunctive* sum of games, that is, a player must choose one heap and make a move in it. The nim-value of a disjunctive sum of games is the nim-sum of the nim-values. This is obtained by writing out the nim-values in binary and adding without carrying, denoted by $\oplus$. The single heap games of Couples-are-Forever have nim-values: $\mathscr{G}(1) = \mathscr{G}(2) = 0$ since these are end-positions. A heap of 3 can be split into heaps of size 1 and 2 so that $\mathscr{G}(3) = \operatorname{mex}\{\mathscr{G}(1) \oplus \mathscr{G}(2)\} = \operatorname{mex}\{0 \oplus 0\} = \operatorname{mex}\{0\} = 1$. Similarly,

$$\begin{aligned}\mathscr{G}(4) &= \operatorname{mex}\{\mathscr{G}(1) \oplus \mathscr{G}(3), \mathscr{G}(2) + \mathscr{G}(2)\}\\ &= \operatorname{mex}\{0 \oplus 1, 0 + 0\} = \operatorname{mex}\{1,0\} = 2.\end{aligned}$$

The first twenty-five nim-values are: 0, 0, 1, 2, 0, 1, 2, 3, 1, 2, 3, 4, 0, 3, 4, 2, 1, 3, 2, 1, 0, 2, 1, 4, 5. By automating the work, we have found the nim-values for heaps of size 1 through 50 million and no pattern has emerged. The value 0 occurs fourteen times

and 1 twenty-six times. The largest nim-value found is $\mathcal{G}(19,739,544) = 325$ and the most common values are:

nim-value:	256	257	129	128	134	135
no. of occurrences:	1,798,261	1,596,606	1,059,556	1,058,974	894,436	893,216

The behavior of the nim-values is quite striking when they are plotted against the heap size. The upper envelope of the graph rises in a linear fashion to approximately 300 at heap size 20,000. Then it is almost constant for the rest of the 50 million terms. A 'sparse-space-common-coset' phenomenon occurs; see [**5**]. A *rare* nim-value in this game is one which has an even number of 1-digits in its binary expansion if the digits in the 'ones' and 'sixteens' places are ignored. Values with an odd number of such 1-digits are called *common*. The nim-sum of two rare values, and likewise of two common values, is a rare value and so rare values tend to get excluded in the mex operation, keeping them rare. This allows for fast calculation of the nim-values: find the smallest common value that does not arise as the nim-sum from heaps, one with a rare value, the other with a common. Then the mex is either this, or is a smaller rare value, so compute sufficient 'common-common' (and 'rare-rare') values until all smaller rare values are excluded, or, exceptionally, you've discovered a new rare value.

If the rare values stop appearing and the sequence of nim-values remains bounded, then it eventually becomes periodic. For Couples-are-Forever, the last rare value found is $\mathcal{G}(20{,}628) = 277$. Unfortunately we cannot prove that there are no more.

Question: *Is Couples-are-Forever ultimately periodic*?

If it is ultimately periodic then the period length cannot divide the size of any heap that has nim-value zero. The nim-value zero occurs for heap sizes 1, 2, 5, 13, 21, 31, 47, 73, 99, 125, 151, 177, 315, and 409, so the period cannot be any of: 1, 2, 3, 5, 7, 9, 11, 15, 21, 25, 31, 33, 35, 45, 47, 59, 63, 73, 99, 105, 125, 151, 177, 315, or 409.

Are there any other reasons to believe that Couples-are-Forever is periodic? Some variants are easily shown to be periodic. If heaps of size 1 through n are not allowed to be split then: the period is $0, 1, 2 \dots, n$ with a pre-period of $n - 1$ zeros if n is odd; the period is $n + 1, 1, 2, \dots, n$ with a pre-period of n zeros followed by $1, 2, \dots, n, 1, 2, \dots, n + 1, 1, 2, \dots, n + 1, 1, 2, \dots, n - 1, 0$ if $n = 2^k - 4$ for $k \geq 3$. However, the other values of n give games as intransigent as the original; see [**3**] for other results.

Couples-are-Forever is very similar to *Grundy's Game* (split a heap into two *unequal* heaps) in that the game ends with heaps of just one or two. This also defies analysis, in spite of several energetic attempts. It was during his computation of the first quarter million nim-values that Elwyn Berlekamp discovered the sparse-space-common-coset phenomenon (see [**2**, p. 111]); here the sparse space comprises vectors of even weight after deleting the units digit. The 1,272nd rare value is $\mathcal{G}(36{,}184) = 157$ and then, apart from $\mathcal{G}(82{,}860) = 108$, no more. Nor did Mike Guy find any more among the first ten million. But Anil Gangolli found $\mathcal{G}(47{,}468{,}481) = 261$, $\mathcal{G}(48{,}142{,}376) = 265$ and 11 other rare values between. Dan Hoey has reached 11 billion, but found neither a pattern nor any more rare values.

Wild conjecture: *All finite octal games are ultimately periodic.*

An *octal game* is a 'take-and-break' game with Guy-Smith code [6] $.\mathbf{d}_1\mathbf{d}_2\mathbf{d}_3\ldots$, where the base 8 digits $\mathbf{d}_i = 2^2h_{i2} + 2^1h_{i1} + 2^0h_{i0}$ with $h_{ij} = 1$ or 0, signify that you may(1) or may not(0) take i counters from a heap, provided that you leave exactly j nonempty heaps in its place. For example, in the game **.172**, you may take one counter if it's on its own, two counters in any case, leaving the remainder, if any, in one or two heaps, or three counters from a heap provided that it is not the whole heap. The analysis of this game has not been completed, nor has it for Officers, **.6** (take one counter from a larger heap, leaving the rest as one or two heaps), nor for **.007** (Treblecross or one-dimensional tic-tac-toe; remove three contiguous skittles from a row), nor for any of the following games ([7, pp. 475–476], where **.644** should not appear, since its period length, 442, was discovered by Richard Austin [1]): **.06, .14, .36, .64, .74, .76, .004, .005, .006, .016, .104, .106, .114, .135, .136, .142, .143, .146, .162, .163, .324, .336, .342, .362, .371, .374, .404, .414, .416, .444, .454, .564, .604, .606, .744, .764, .774, .776**, and plenty of games where you're allowed to take more than three counters.

We return to the splitting games. A *pure* period is a sequence of numbers $(a_1, a_2, \ldots, a_k)$ where

$$a_j = \operatorname{mex}\left\{a_i \oplus a_{j-i} | i = 1, 2, \ldots, k-1, \quad \text{where the subscripts are taken cyclically}\right\}.$$

When a pure period exists, the corresponding splitting game has $\mathscr{G}(n)$ prescribed for $n = 1, 2, \ldots, k$ and thereafter, $\mathscr{G}(n+k) = \mathscr{G}(n)$. For example, 0 1 is a pure period. There are pure periods $2^n\ 3^2\ 2^n\ 1$ of length $2n+3$, and $1\ (3\ 0)^n\ 3\ 1\ 1$ of length $2n+4$, for every $n \geq 1$, where $(*)^n$ means $*$ repeated n times.

A pure period of length k can have no value greater than $\lfloor k/2 \rfloor$, since there are only $\lceil k/2 \rceil$ terms when taking the *mex* and one of the terms must be zero for the maximum nim-value to occur. We have calculated all pure periods up to length 11, of which there are many.

For period lengths one through eleven, there are 1, 2, 1, 2, 3, 6, 7, 18, 13, 58, 50 pure periods respectively. All have the form $SS^{-1}1$ if of odd length and $SaS^{-1}1$ if even, where S^{-1} is the sequence S in reverse and a is a single number.

What finite sequences of nim-values are pure periods? Must they have the form $SaS^{-1}1$ *or* $SS^{-1}1$?

REFERENCES

1. Richard Bruce Austin, *Impartial and partisan games*, M.Sc. thesis, The Univ. of Calgary, 1976.
2. E. R. Berlekamp, J. H. Conway, and R. K. Guy, *Winning Ways for Your Mathematical Plays*, Academic Press, London, 1982.
3. I. Caines, C. Gates, and R. J. Nowakowski, Binary splitting games, 1998 manuscript.
4. J. H. Conway, *On Numbers and Games*, Academic Press, London, 1976.
5. Anil Gangolli and Thane Plambeck, A note on periodicity in some octal games, *Internat. J. Game Theory* **18** (1989) 321–325.
6. Richard K. Guy and Cedric A. B. Smith, The G-values for various games, *Proc. Cambridge Philos. Soc.*, **52** (1956) 514–526; *MR* **18**, 546.
7. Richard J. Nowakowski (editor), *Games of No Chance*: *Combinatorial Games at MSRI*, 1994, Math. Sci. Res. Inst. Publications **29**, Cambridge University Press, 1996.

Dalhousie University, Halifax, Nova Scotia, Canada, B3H 3J5.
ian.caines@dal.ca; carrie.gates@dal.ca; rjn@mscs.dal.ca

University of Calgary, Calgary, Alberta, Canada T2N 1N4
rkg@cpsc.ucalgary.ca

PROBLEMS AND SOLUTIONS

Edited by **Gerald A. Edgar, Daniel H. Ullman,** and **Douglas B. West**

with the collaboration of Paul T. Bateman, Mario Benedicty, Paul Bracken, Duane M. Broline, Ezra A. Brown, Richard T. Bumby, Glenn G. Chappell, Randall Dougherty, Roger B. Eggleton, Ira M. Gessel, Bart Goddard, Jerrold R. Griggs, Douglas A. Hensley, Richard Holzsager, John R. Isbell, Robert Israel, Kiran S. Kedlaya, Murray S. Klamkin, Fred Kochman, Frederick W. Luttmann, Vania Mascioni, Frank B. Miles, Richard Pfiefer, Cecil C. Rousseau, Leonard Smiley, John Henry Steelman, Kenneth Stolarsky, Richard Stong, Charles Vanden Eynden, and William E. Watkins.

Proposed problems and solutions should be sent in duplicate to the MONTHLY *problems address on the inside front cover. Submitted problems should include solutions and relevant references. Submitted solutions should arrive at that address before September 30, 1999; Additional information, such as generalizations and references, is welcome. The problem number and the solver's name and address should appear on each solution. An acknowledgement will be sent only if a mailing label is provided. An asterisk (*) after the number of a problem or a part of a problem indicates that no solution is currently available.*

PROBLEMS

10725. *Proposed by Vasile Mihai, Toronto, ON, Canada.* Fix a positive integer n. Given a permutation α of $\{1, 2, \ldots, n\}$, let $f(\alpha) = \sum_{i=1}^{n}\big(\alpha(i)-\alpha(i+1)\big)^2$, where $\alpha(n+1) = \alpha(1)$. Find the extreme values of $f(\alpha)$ as α ranges over all permutations of $\{1, 2, \ldots, n\}$.

10726. *Proposed by Donald E. Knuth, Stanford University, Stanford, CA.* Start in state 0. For every nonnegative integer k, stay in state k for X_k units of time, then go to state $k+1$. What is the probability of being in state s after t units of time, assuming that X_k is distributed exponentially **(a)** with mean $1/(k+1)$? **(b)** with mean $1/2^k$?

10727. *Proposed by Jean Anglesio, Garches, France.* Let m be a fixed positive integer. For a positive integer n, let $s_m(n)$ be the sum of the mth powers of the decimal digits of n. For example, $s_3(172) = 1^3 + 7^3 + 2^3 = 352$. Starting with any positive integer n_0, construct a sequence of positive integers by setting $n_k = s_m(n_{k-1})$ for every $k \geq 1$.

(a) Show that $n_0, n_1, n_2, \ldots$ is eventually periodic.

(b) Show that only finitely many periods are possible as n_0 varies.

10728. *Proposed by Titu Andreescu, American Mathematics Competitions, Lincoln, NE.* Determine all functions $f\colon \mathbb{Z} \to \mathbb{Z}$ satisfying

$$f(x^3 + y^3 + z^3) = \big(f(x)\big)^3 + \big(f(y)\big)^3 + \big(f(z)\big)^3$$

for all integers x, y, and z.

10729. *Proposed by David P. Bellamy and Felix Lazebnik, University of Delaware, Newark, DE.* Let $I \subset \mathbb{R}$ be an open interval, and let n be a positive integer. Characterize the functions $f\colon I \to \mathbb{R}$ that have a continuous nth derivative and satisfy

$$f^{(n)} + p_1 f^{(n-1)} + \cdots + p_{n-1} f' + p_n f = 0$$

for some continuous functions $p_1, p_2, \ldots, p_n$ on I.

10730. *Proposed by Walther Janous, Ursulinengymnasium, Innsbruck, Austria.* Fix an integer $n \geq 2$. Determine the largest constant $C(n)$ such that

$$\sum_{1 \leq i < j \leq n} (x_j - x_i)^2 \geq C(n) \cdot \min_{1 \leq i < n} (x_{i+1} - x_i)^2$$

for all real numbers $x_1 < x_2 < \cdots < x_n$.

10731. *Proposed by M. J. Pelling, London, England.* Let A be an n-by-n real symmetric matrix, and consider the quadratic form $Q(x) = x^T Ax$ for $x \in \mathbb{R}^n$. Let C be the cube $[-1, 1]^n$. Prove that $\max_{x \in C} Q(x)$ is at least as large as the sum of the positive real eigenvalues of A.

SOLUTIONS

Connected Sets of Periodic Functions

10434 [1995, 170]. *Proposed by Daniel Goffinet, Saint Étienne, France.* Let P be the set of nonconstant periodic mappings from $\mathbb{R}$ to $\mathbb{R}$, endowed with the topology derived from the supremum norm. Find the components of P.

Composite solution I by Kiran S. Kedlaya, Massachusetts Institute of Technology, Cambridge, MA, Kenneth Schilling, University of Michigan, Flint, MI, and Arlo W. Schurle, University of Guam, Mangilao, Guam. For any function $f: \mathbb{R} \to \mathbb{R}$, define $\|f\|$ to be $\sup\{ |f(x)| : x \in \mathbb{R}\}$, which is taken to be ∞ when the set of values of f is unbounded.

We first show that f and g are in different components of P if $\|f - g\| = \infty$. Let $B_g = \{ k \in P\colon \|k - g\| < \infty\}$. By the triangle inequality B_g is an open set, and if $h \notin B_g$, then the triangle inequality again shows that $\{ z\colon \|z - h\| < 1\} \cap B_g = \emptyset$. Consequently B_g is both open and closed, and so the component of P containing any given $g \in P$ must lie in B_g.

Conversely, if $f - g$ is bounded for $f, g \in P$, then there is an arc in P joining f to g. First, suppose that f and g have a common period p. The standard path $k_t(x) = (1 - t)f(x) + tg(x)$ for $0 \leq t \leq 1$ consists of functions having p as a period, and since $\|f - g\|$ is finite, k_t depends continuously on t. There is a danger that some $k_t(x)$ is a constant function, but this can happen only if f is an affine function of g, that is, there are constants A and B with $f = Ag + B$. In this case, the function $h(x)$ that is equal to $f(x)$ except at integer multiples of p, where it is $f(x) + 1$, is at bounded distance from both f and g and is not an affine function of either. A path from f to g can be obtained by taking the standard path from f to h followed by the standard path from h to g.

Suppose now that f and g have no common period. Let r be a period of f and let s be a period of g. We wish to construct h that has both r and s as periods such that $\|f - h\|$ (and hence also $\|g - h\|$) is finite. To do this, pick an arbitrary set of coset representatives for $\mathbb{R}/(r\mathbb{Z} + s\mathbb{Z})$, define h to agree with f at these values, and extend by periodicity. Then for any x, let $x = y + rm + sn$, where y represents the coset containing x. Then

$$\begin{aligned} |h(x) - f(x)| &= |f(y) - f(y + sn)| \\ &= |f(y) - g(y) + g(y + sn) - f(y + sn)| \leq 2\,\|f - g\| \end{aligned}$$

Since f and h have common period r and $\|f - h\|$ is finite, there is a path from f to h, and since h and g have common period s and $\|h - g\|$ is finite, there is a path from h to g.

Composite solution II by Fredric D. Ancel, University of Wisconsin, Milwaukee, WI, Phil Bowers and John Bryant, The Florida State University, Tallahassee, FL, and the proposer. We assume that "mapping" means "continuous function". Then two functions in P belong to the same component if and only if they have commensurate periods. As in solution I, the components are path-components.

Given $f \in P$ with period $2\pi n$, we form a path from $f(x)$ to $\sin x$ via the homotopy $h_t(x) = (1-t)f(x)+t\sin x$ for $0 \le t \le 1$. Since $\|h_s - h_t\| \le \big(\|f\|+1\big)|s-t|$, the map $t \mapsto h_t$ is continuous from $[0, 1]$ to the space of all functions from $\mathbb{R}$ to $\mathbb{R}$ with the topology derived from the supremum norm. Each h_t has $2n\pi$ as a period. This gives the desired path in P if no $h_t(x)$ is constant, i.e., unless $f(x) = A\sin x + B$ with $A < 0$. For such $f(x)$, the path $k_t(x) = (1-t)f(x) - t\sin x$ connects $f(x)$ to $-\sin x = \sin(x+\pi)$. The path $n_t(x) = \sin(x + (1-t)\pi)$ then connects $-\sin x$ to $\sin x$ in P. The continuity of $t \mapsto n_t$ follows from the mean value theorem. If f and g have commensurate periods, say both are a multiple of p, then there are continuous paths in P connecting $f(x)$ to $\sin(2\pi x/p)$ and $g(x)$ to $\sin(2\pi x/p)$, hence there is a path from f to g.

For a fixed real number p, let C_p denote the set of functions in P whose period is a rational multiple of p. We now show that C_p is an open subset of P. Choose $f \in C_p$. Since f is not constant, there are real numbers x and y such that $f(x) < f(y)$. Set $\epsilon = \big(f(y) - f(x)\big)/3$. We show that $g \in P$ and $\|f - g\| < \epsilon$ implies $g \in C_p$. If not, then there is g with $\|f - g\| < \epsilon$ such that the period of g, say q, is an irrational multiple of p. Since f is continuous, there is δ such that f takes the interval $(y-\delta, y+\delta)$ into the interval $(f(y)-\epsilon, f(y)+\epsilon)$. Since $f \in C_p$, f also takes the interval $(y - mp - \delta, y - mp + \delta)$ into $(f(y) - \epsilon, f(y) + \epsilon)$ for each integer m. Since $\|f - g\| < \epsilon$, g takes each $(y - mp - \delta, y - mp + \delta)$ into $(f(y) - 2\epsilon, f(y) + 2\epsilon)$. Since p/q is irrational, the numbers $mp + nq$ for integers m and n are dense in $\mathbb{R}$, so there are integers m and n such that $mp+nq \in (y - x - \delta, y - x + \delta)$, which gives $x + nq \in (y - mp - \delta, y - mp + \delta)$. Thus, $g(x + nq) < f(x) + \epsilon = f(y) - 2\epsilon < g(x+nq)$, a contradiction. This completes the proof that C_p is an open subset of P.

Since the sets C_p partition P into connected open sets, each set C_p is a component of P.

The Plane Covered by Disks

10440 [1995, 273]. *Proposed by Marius Cavachi, Constanta, Romania.* Show that the Euclidean plane cannot be covered with circular disks having mutually disjoint interiors.

Solution I by Sam Northshield, SUNY, Plattsburgh, NY. We show that $\mathbb{R}^k$ $(k \ge 2)$ cannot be covered by metric balls having mutually disjoint interiors.

Note that every set of balls with disjoint interiors is countable, since each contains a different point with rational coordinates. Let $\{B_n\colon n \in \mathbb{N}\}$ be a set of closed metric balls in $\mathbb{R}^k$ $(k \ge 2)$ with mutually disjoint interiors. A point of intersection of two of the B_n is called an *intersection point.* Since the intersection of two distinct B_n has at most one point, there are only countably many intersection points. Hence we may choose a straight line segment γ with its endpoints in the interiors of two distinct balls and such that γ avoids all intersection points (here is where we need $k \ge 2$). Let C be the set of points of γ that are *not* in the interior of any B_n. Then C is closed and nonempty. Furthermore, any neighborhood of point $x \in C$ must contain another point of C; otherwise x would be an intersection point. Hence C is perfect, and thus uncountable. Now, for any n, the segment γ intersects ∂B_n in at most two points, so there is $x \in C$ not in any B_n. It follows that $\bigcup B_n \neq \mathbb{R}^k$.

Solution II by Simeon T. Stefanov, Sofia, Bulgaria. Suppose the contrary. As in Solution I, there are only countably many intersection points. Let L be a line that avoids these points, and consider the family $\mathcal{F} = \{L \cap B_n\colon n \in \mathbb{N}\}$, a countable cover of L with disjoint closed bounded intervals. To see that no such cover is possible, construct a nested family of compact intervals $\Delta_n \subseteq L$ such that $\Delta_n \cap B_n = \emptyset$, but Δ_n meets at least two intervals in $\mathcal{F}$. Then $\bigcap \Delta_n$ is nonempty, but no point of this intersection belongs to any set in $\mathcal{F}$.

Editorial comment. Victor Klee noted that the proof that there are only countably many intersection points requires only that the B_n be *rotund* (i.e., strictly convex). His solution followed Solution II, with the last part traced back to W. Sierpiński, Un théorème sur les

continus, *Tôhoku Mat. J.* 13 (1918) 300–303. Klee also noted that circular disks are *smooth* (i.e., possess a continuously differentiable parameterization) as well as rotund. For more on smooth tilings, see V. Klee, E. Maluta, and C. Zanco, Tiling with smooth and rotund tiles, *Fund. Math.* 126 (1986) 269–290; V. Klee and C. Tricot, Locally countable plump tilings are flat, *Math. Ann.* 277 (1987) 315–325; and P. M. Gruber, How well can space be packed with smooth bodies? Measure theoretic results, *J. London Math. Soc.* (2) 52 (1995) 1–14.

D. G. Larman, A note on the Besicovich dimension of the closest packing of sphere in R_n, *Proc. Cambridge Philos. Soc.* 62 (1966) 193–195 shows that, in the case of packing of circular disks in the plane, the uncovered set has Hausdorff dimension at least 1.03.

Solved also by G. E. Bredon, P. Budney, J. D. Clemens, J. Cobb, R. Holzsager, A. A. Jagers (The Netherlands), V. Klee, J. H. Lindsey II, O. P. Lossers (The Netherlands), R. Martin (Germany), L. E. Mattics, M. Misiurewicz, I. Namioka, O. Nanyes, C. G. Petalas & T. P. Vidalis (Greece), C. Popescu (Belgium), A. W. Schurle, J. H. Shapiro & T. L. McCoy, A. A. Tarabay & R. Barbara (Lebanon), and the Anchorage Math Solutions Group.

Random Perfect Matchings

10587 [1997, 361]. *Proposed by Joaquín Gómez Rey, Madrid, Spain.* Let K_{2n} be the complete graph on $2n$ vertices. Let P_n be the probability that two random perfect matchings of K_{2n} are disjoint. What is $\lim_{n\to\infty} P_n$?

Solution by José Heber Nieto, Universidad del Zulia, Maracaibo, Venezuela. The limit is $e^{-1/2} \approx 0.60653$. The number of perfect matchings of K_{2n} is $M_n = (2n)!/(2^n n!)$. Given a perfect matching G of K_{2n} and a set J of j edges of G, there are M_{n-j} perfect matchings of K_{2n} containing J. Therefore, the inclusion-exclusion principle yields $\sum_{j=0}^{n}(-1)^j\binom{n}{j}M_{n-j}$ as the number of perfect matchings of K_{2n} disjoint from G. Thus

$$P_n = \sum_{j=0}^{n}(-1)^j\binom{n}{j}\frac{M_{n-j}}{M_n}.$$

Now $\lim_{n\to\infty} P_n$ can be computed by applying Lebesgue's dominated convergence theorem. Let $X = \{0, 1, 2, \ldots\}$, and define a measure μ on X by $\mu(\{j\}) = 1/j!$. Let $f_n: X \to \mathbb{R}$ be defined by

$$f_n(j) = \frac{(-1)^j n! M_{n-j}}{(n-j)! M_n} = (-1)^j \prod_{i=0}^{j-1} \frac{n-i}{2n-2i-1}.$$

Then $\lim_{n\to\infty} f_n(j) = (-1/2)^j$. Furthermore, $|f_n(j)| \le 1$, and the constant function 1 is integrable, since $\int_X 1\,d\mu = \sum_{j=0}^{\infty} 1/j! = e$. Therefore,

$$\lim_{n\to\infty} P_n = \lim \int_X f_n\,d\mu = \int_X \lim f_n\,d\mu = \sum_{j=0}^{\infty}\frac{(-1/2)^j}{j!} = e^{-1/2}.$$

Solved also by R. J. Chapman (U. K.), R. DiSario, J. Grossman, J. Labelle, D. Tenny, NCCU Problems Group, and the proposer.

Characterizations of the Medial Triangle

10588 [1997, 361]. *Proposed by Marcin Mazur, The University of Chicago, Chicago, IL.* Let $A_1A_2A_3$ be a triangle. For $i = 1, 2, 3$, let B_i be a point on side $A_{i+1}A_{i+2}$, where subscripts are taken modulo 3.

(**a**) Show that $|A_iB_{i+1}| + |B_iB_{i+1}| = |A_iB_{i+2}| + |B_iB_{i+2}|$ for $i = 1, 2, 3$ if and only if B_i is the midpoint of $A_{i+1}A_{i+2}$ for $i = 1, 2, 3$.

(**b**) Show that $|A_iB_{i+1}| + |A_iB_{i+2}| = |B_iB_{i+1}| + |B_iB_{i+2}|$ for $i = 1, 2, 3$ if and only if B_i is the midpoint of $A_{i+1}A_{i+2}$ for $i = 1, 2, 3$.

Solution by the proposer. If B_i is the midpoint of $A_{i+1}A_{i+2}$ for $i = 1, 2, 3$, then triangles $A_1A_2A_3$ and $B_1B_2B_3$ are similar, so $|B_1B_2| = (1/2)|A_1A_2|$, $|B_2B_3| = (1/2)|A_2A_3|$, and $|B_3B_1| = (1/2)|A_3A_1|$. Hence

$$|A_1B_2| + |B_1B_2| = \frac{1}{2}|A_1A_3| + \frac{1}{2}|A_1A_2| = |B_1B_3| + |A_1B_3|,$$

and similarly for the other conditions of both parts.

(**a**) We prove that for any triangle $B_1B_2B_3$ there exists exactly one triangle $A_1A_2A_3$ such that $|A_iB_{i+1}|+|B_iB_{i+1}| = |A_iB_{i+2}|+|B_iB_{i+2}|$ for $i = 1, 2, 3$. This implies our assertion. Fix a triangle $B_1B_2B_3$, and suppose that for a triangle $A_1A_2A_3$ the conditions are satisfied. Let (i, j, k) be a permutation of $(1, 2, 3)$. Consider the hyperbola with foci B_j and B_k passing through B_i. Since $|A_iB_j| + |B_iB_j| = |A_iB_k| + |B_iB_k|$, the hyperbola passes through A_i. Write h_i for the part of the branch of the hyperbola passing through A_i that is on the opposite side of the line B_jB_k from B_i. Since B_j and B_k are the foci of the hyperbola, h_i is entirely contained in the union of all lines joining A_i and some point on the segment B_jB_k.

Now suppose that A is any point on h_1 different from A_1. (This A is a candidate for the vertex A_1 in a new triangle satisfying the conditions.) If A is inside triangle $B_2A_1B_3$, then the line from A through B_2 intersects h_3 in a point P that is on the opposite side of the line A_2A_3 from A_1, and if A is outside of $B_2A_1B_3$ then P is on the same side of A_2A_3 as A_1. (Point P is the candidate for point A_3 of the new triangle.) The same holds for the intersection Q of the line AB_3 with h_2 (the candidate for A_2 of the new triangle). Therefore, the line segment PQ does not pass through B_1. We conclude that A cannot be a vertex of a triangle that satisfies our requirements. A similar argument shows that no point A outside triangle $B_2A_1B_3$ can be a vertex of a triangle that satisfies our requirements. Thus $A_1A_2A_3$ is the only triangle for which the conditions hold.

(**b**) Let $a_k = (1/2)|A_iA_j|$, $b_k = |B_iB_j|$, and $x_j = a_j - |A_iB_j|$, where (i, j, k) is an even permutation of $(1, 2, 3)$. By hypothesis, $a_i + x_i + a_k - x_k = b_i + b_k$. Adding two of these equations and subtracting the third yields $b_i = a_i - x_j + x_k$, so

$$b_i^2 = a_i^2 + x_j^2 + x_k^2 - 2a_ix_j - 2x_jx_k + 2a_ix_k \tag{1}$$

By the law of cosines we obtain $b_i^2 = (a_j + x_j)^2 + (a_k - x_k)^2 - 2(a_j + x_j)(a_k - x_k)\cos A_i$. Since $\cos A_i = a_j^2 + a_k^2 - a_i^2/2a_ja_k$ we get after simple transformations

$$b_i^2 = a_i^2 + x_j^2 + x_k^2 + \frac{x_j}{a_j}(a_j^2 + a_i^2 - a_k^2) - \frac{x_k}{a_k}(a_k^2 + a_i^2 - a_j^2) + \frac{x_j}{a_j}\frac{x_k}{a_k}(a_j^2 + a_k^2 - a_i^2) \tag{2}$$

Let $z_i = x_i/a_i$. Comparing expressions (1) and (2) for b_i^2, we get

$$z_j(a_j + a_i - a_k) - z_k(a_k + a_i - a_j) + z_jz_k(a_j + a_k - a_i) = 0\,.$$

If one of the z_i's is 0, then all of them vanish. If they are all nonzero, then dividing by z_jz_k and adding all three equalities we get $a_1 + a_2 + a_3 = 0$, which is evidently false. Therefore, all the x_i's vanish and the assertion is proved.

Solved also by M. Vowe (Switzerland) and GCHQ Problems Group (U. K.).

Binary Expansions and kth Powers

10596 [1997, 456]. *Proposed by Paul Bateman, University of Illinois, Urbana, IL, and David Bradley, Simon Fraser University, Burnaby, BC, Canada.*

(**a**) Prove the identity

$$\sum_{j=0}^{2^{k-1}-1} (-1)^{k-1-\eta(j)}(y + j)^k = k! \cdot 2^{(k-1)(k-2)/2}(y + (2^{k-1} - 1)/2),$$

where $\eta(j)$ is the number of ones in the binary expansion of the nonnegative integer j.
(b) Use part **(a)** to infer that there is a positive integer $s = s(k)$ such that every integer n is expressible in the form $n = \epsilon_1 x_1^k + \epsilon_2 x_2^k + \cdots + \epsilon_s x_s^k$ in infinitely many ways, where $\epsilon_i = \pm 1$ for $1 \le i \le s$ and where $x_1, x_2, \ldots, x_s$ are distinct positive integers.

Solution I to part **(a)** *by David Callan, University of Wisconsin, Madison, WI.* With $n = k-1$, equating coefficients of y reduces the proposed identity to

$$\sum_{j=0}^{2^n-1} (-1)^{n-\eta(j)} j^r = \begin{cases} 0 & \text{if } r < n; \\ n!2^{n(n-1)/2} & \text{if } r = n; \\ (n+1)!2^{n(n-1)/2}(2^n-1)/2 & \text{if } r = n+1. \end{cases}$$

Let $S(j)$ denote the set of positions containing 1 in the binary representation of j, so that, for example, $S(13) = S((1101)_2) = \{1,3,4\}$). Write $j \preceq k$ when $S(j) \subseteq S(k)$. Consider a set of boxes labeled $1, \ldots, 2^n - 1$. For $0 \le i \le n-1$, let G_i be the set of boxes with labels $2^i, \ldots, 2^{i+1} - 1$. Note that $|G_i| = 2^i$ for $i \ge 0$.

Let $f(j)$ be the number of placements of r distinguishable balls into $\bigcup_{i \in S(j)} G_i$. Clearly $f(j) = j^r$. Let $g(j)$ be the number of such placements in which, for each $i \in S(j)$, at least one ball is in at least one box in G_i. By the Inclusion-Exclusion Principle, $g(k) = \sum_{j \preceq k} (-1)^{\eta(k)-\eta(j)} f(j)$. In particular, $g(2^n-1) = \sum_{j=0}^{2^n-1} (-1)^{n-\eta(j)} j^r$.

Since $S(2^n - 1) = \{1, \ldots, n\}$, the distributions counted by $g(2^n - 1)$ are those with all n groups nonempty. When $r < n$, there are none. When $r = n$, one of the 2^i boxes in G_i is used, for each i. When $r = n+1$, we distribute n balls and then one more, dividing by 2 to eliminate overcounting. Thus both sides of the identity equal $g(2^n - 1)$.

Solution II by Richard Stong, Rice University, Houston, TX.
(a) Letting $\Delta_r f(y) = f(y+r) - f(y)$, the left side of the identity is $\Delta_1 \Delta_2 \Delta_4 \cdots \Delta_{2^{k-2}} y^k$. If f is a polynomial of degree n with leading coefficient c, then $\Delta_r f$ is a polynomial of degree $n-1$ with leading coefficient crn. Since we have applied $k-1$ such operators, the left side of the identity is a polynomial of degree 1 with leading coefficient $k!2^{0+1+\cdots+(k-2)} = k!2^{(k-1)(k-2)/2}$.

Since $\eta(2^{k-1} - 1 - i) = k - 1 - \eta(i)$, the terms for $j = i$ and $j = 2^{k-1} - 1 - i$ in the sum exactly cancel if $y = -(2^{k-1} - 1)/2$. Thus the left side of the identity is the polynomial of degree 1 with leading coefficient $k!2^{(k-1)(k-2)/2}$ that vanishes at $y = -(2^{k-1} - 1)/2$. This agrees with the right side.
(b) If $k = 1$, then $s = 3$ suffices, because the identities $n = (n+2+m) - (1+m) - 1$ and $n = (m+2+n) - (m+1-n) - (1-n)$ give suitable representations for all $m \ge 1$ in the cases $n \ge 0$ and $n < 0$, respectively.

Now consider $k \ge 2$. Let $M = k!2^{(k-1)(k-2)/2}$, and let $s(k) = M + 2^{k-1}$. Given any integer n, choose integers q and r such that $n = (2^{k-1} - 1)M/2 + Mq + r$, where $0 \le r < M$. Let $x_1, \ldots, x_r$ be multiples of M, and let $x_{r+1}, \ldots, x_M$ be numbers congruent to 1 modulo M. Now $n + \sum_{i=1}^M x_i^k$ is congruent to $(2^{k-1} - 1)M/2$ modulo M. Thus for some y we have $n + \sum_{i=1}^M x_i^k = M(y + (2^{k-1} - 1)/2)$. The identity in **(a)** now yields

$$n = \sum_{j=0}^{2^{k-1}-1} (-1)^{k-1-\eta(j)} (y+j)^k - \sum_{i=1}^M x_i^k.$$

The numbers $x_1, \ldots, x_M$ were chosen arbitrarily subject to congruence conditions modulo M; there are infinitely many such choices. By fixing $x_1, \ldots, x_{M-1}$ and making x_M sufficiently large, we can ensure that y exceeds x_M, since $k \ge 2$. Thus we have infinitely many choices in which $x_1, \ldots, x_M, y, y+1, \ldots, y + 2^{k-1} - 1$ are distinct, as desired.

Solved also by K. McInturff, J. H. Lindsey II, GCHQ Problems Group (U. K.), R. J. Chapman (U. K.), and the proposers. Part **(a)** solved also by D. Beckwith.

A Supremum of Sine Differences

10604 [1997, 567]. *Proposed by Joseph Rosenblatt, University of Illinois, Urbana, IL.*
(a) Determine positive constants c and C such that if $0 < a < b$ then

$$c\left(1-\frac{a}{b}\right) \le \sup_{x>0}\left|\frac{\sin(ax)}{ax} - \frac{\sin(bx)}{bx}\right| \le C\left(1-\frac{a}{b}\right). \qquad (*)$$

(b)* What are the largest constant c and smallest constant C such that $(*)$ holds whenever $0 < a < b$?

Solution of part **(a)** *by Thomas Hermann, SDRC, Milford, OH.* We may take $c = 2/\pi$ and $C = 4$. To see this, let $\varphi(x) = \sin x/x$, $\lambda = a/b$, and $\mu(\lambda, x) = \big(\varphi(x) - \varphi(\lambda x)\big)/(1-\lambda)$. The problem is to find positive lower and upper bounds for $M(\lambda) = \sup_{x>0} |\mu(\lambda, x)|$. Since $|\varphi(x)| \le 1$ for all x,

$$|\mu(\lambda, x)| \le \frac{2}{1-\lambda} \le 4 \qquad (1)$$

when $0 < \lambda \le 1/2$. By the Mean Value Theorem, there is a $y \in [\lambda x, x]$, such that $\mu(\lambda, x)/x = \varphi'(y)$. Now $x\varphi'(y) = (x/y)(\cos y - \varphi(y))$, so

$$|\mu(\lambda, x)| \le 2\,\frac{x}{y} \le \frac{2}{\lambda} \le 4 \qquad (2)$$

when $\frac{1}{2} \le \lambda < 1$. Combining (1) and (2), we obtain $M(\lambda) \le 4$ for all λ in $(0, 1)$.

To get a lower bound, observe that $\mu(\lambda, \pi) = \sin(\lambda\pi)/\left(\lambda(1-\lambda)\pi\right) = \mu(1-\lambda, \pi)$, so it is enough to consider the case when $\lambda \in (0, 1/2]$. Since $\varphi(x)$ is decreasing on $(0, \pi/2]$, $\mu(\lambda, \pi) \ge \big(1/(1-\lambda)\big)\big(\sin(\pi/2)/(\pi/2)\big) \ge 2/\pi$. Therefore $2/\pi \le M(\lambda) \le 4$.

Editorial comment. For part **(b)**, John H. Lindsey II and the GCHQ Problems Group independently computed that the largest value for c is approximately 1.0631036 and the smallest value for C is approximately 1.3805662. Lindsey used Maple to search for these values and used estimates on derivatives to prove that the optimal value of C satisfies $1.380566167 \le C \le 1.380577012$.

Part (a) also solved by R. J. Chapman (U.K.), T. Hermann, J. H. Lindsey II, GCHQ Problems Group (U.K.), and the proposer.

A Convergent Series

10657 [1998, 366]. *Proposed by Jovan Vukmirović, University of Belgrade, Belgrade, Yugoslavia.* Let ϕ be a strictly increasing function from $(0, \infty)$ onto $(0, \infty)$. Prove that if $\sum_{n=1}^{\infty} 1/(n\phi^{-1}(n))$ converges, then $\sum_{n=1}^{\infty} \phi(n)x^n$ converges for $|x| < 1$.

Solution by Kenneth Schilling, University of Michigan, Flint, MI. For $x > 1$,

$$\sum_{n=\lfloor\sqrt{x}\rfloor}^{\lfloor x\rfloor} \frac{1}{n} > \int_{\sqrt{x}}^{x} \frac{1}{t}\,dt = \frac{1}{2}\ln x.$$

Thus, since ϕ is increasing, we have

$$\frac{\ln x}{2\phi^{-1}(x)} < \sum_{n=\lfloor\sqrt{x}\rfloor}^{\lfloor x\rfloor} \frac{1}{n\phi^{-1}(x)} < \sum_{n=\lfloor\sqrt{x}\rfloor}^{\lfloor x\rfloor} \frac{1}{n\phi^{-1}(n)}.$$

By hypothesis, this expression converges to 0 as $x \to \infty$. Hence $\lim_{x\to\infty} \ln x/\phi^{-1}(x) = 0$. Since $\phi(x) \to \infty$ as $x \to \infty$, we get $\lim_{x\to\infty} \ln\phi(x)/x = 0$. Exponentiation yields $\lim_{x\to\infty}(\phi(x))^{1/x} = 1$. Thus the power series converges for $|x| < 1$ by the root test.

Solved also by S. Amghibech (France), J. Arregui, G. L. Body (U. K.), D. Borwein (Canada), D. Bradley (Canada), K. Dale & I. Skau (Norway), J. Fitch, K. Ford, G. L. Isaacs, P. Lang, J. H. Lindsey II, A. Stenger, T. V. Trif (Romania), T. Trimble, R. Vermes (Canada), C. Y. Yildirim (Turkey), GCHQ Problems Group (U. K.), and the proposer.

REVIEWS

Edited by **Harold P. Boas**

Mathematics Department, Texas A & M University, College Station, TX 77843-3368

The French Mathematician. By Tom Petsinis. Walker and Company, New York, 1998, v + 426 pp., $24.

Reviewed by **Tony Rothman**

It is not uncommon in our society for a celebrity to read a novel, recognize herself in one of the characters, and sue the author for defamation. The plaintiff's position in such cases is surely peculiar: On the one hand she must argue that the offending character is real; on the other hand, she must argue that the character is not real enough. While reading Tom Petsinis's new novel about Evariste Galois, one wonders throughout whether Galois would be pleased with this portrait or would call his lawyer. Galois is not forthcoming. As his advocate I would be tempted to advise him to call not a lawyer, I think, but a book doctor. However, this case is one for the jury to decide.

Galois's life, straddling as it did fact and fiction, naturally lends itself to novelization. Most mathematicians and scientists are familiar with the outlines of the story. A mathematical prodigy, Galois came of age in the aftermath of the Napoleonic empire. He twice failed the entrance examination to the prestigious École Polytechnique, where he expected to study mathematics, and enrolled in the École Normale, only to be expelled as a revolutionary firebrand. Arrested on two occasions for seditious activities in the wake of the 1830 revolution, he spent eight months in prison, was released in April 1832 on the advent of the great cholera epidemic, and a month later managed to get himself mortally wounded in a duel. The night before, he wrote out his scientific last will and testament, annotated his papers, and bequeathed his legacy—group theory—to the world. He was twenty years old.

One of the great romances of science, Galois's life has been the inspiration for a dozen novels, plays, and films. My own 1982 MONTHLY article **[4]** was actually the outcome of research for a play about Galois and the Russian poet Pushkin, whose life followed a similar trajectory. Petsinis has evidently followed the general outline of my article. Gone is the Galois of E. T. Bell's *Men of Mathematics* **[1]**, who is done in by the massed forces of stupidity arrayed against him and the shadowy political intrigues of Bell's imagination. Gone also is Leopold Infeld's Galois, hero of the proletariat. Vanished as well is Infeld's pretense that his book **[3]** is actually a work of "faction," a nonfiction novel. No, Petsinis has written a work of fiction, and he has no obvious ax to grind. He has attempted to portray a troubled youth living in turbulent times, a victim as much of his own personality as of external misfortunes. *The French Mathematician* aspires to be a believable portrait, both psychologically and historically.

It is personally gratifying to see one's work transmogrified and so transformed passed into the future, and as a rule one should review the work that has been

created, not the one that hasn't been created. Nevertheless, my feeling on putting down *The French Mathematician* remains that Petsinis might have done better to pen a different book. I am not speaking of historical accuracy. There are many points one can quibble with—the book jacket copy gets the age of Galois at his death wrong, which does little to instill confidence; the ages of Galois's instructors are incorrect, and so on. I may myself have misled Petsinis about Galois's opponent in the celebrated duel. In my MONTHLY article I followed Alexandre Dumas, who stated that Galois's opponent was Pescheux D'Herbinville, a fellow republican. D'Herbinville figures here as Galois's adversary, though thankfully no dark plots, agents provocateur, or prostitutes are invoked, merely jealousy and honor. Well before the 1989 version of my article **[5]**, however, I had been informed of the work of André Dalmas **[2]**, who presents a clipping from a Lyon newspaper dated several days after the duel. The clipping identifies Galois's opponent as L. D., initials that do not match any of Galois's acquaintances. Nevertheless, judging from the article, the most probable opponent was Vincent Duchatelet, one of Galois's best friends. The duel itself seems to have been a grisly version of Russian roulette: the adversaries had both fallen in love with the same girl, but "because of their old friendship they could not bear to look at each other and left the decision to blind fate. At point-blank range they were each armed with a pistol and fired. Only one pistol was charged" **[5]**.

No, historical accuracy is not the issue; this is a novel. At issue is verisimilitude—Petsinis strives for it—and literary achievement. Increasingly I am convinced that God does not reside entirely in the details. To the contrary, the success of a work is largely determined by the basic decisions an author makes at the outset, most importantly: What is the book about? But also such large stylistic decisions as: Will the book be told in first or third person? Present or past tense? Petsinis has decided to tell the story from Galois's own perspective. This decision results in a threefold hurdle that is almost impossible to surmount: He must get inside the head of an adolescent; he must get inside the head of an early 19th-century adolescent; and he must get inside the head of an early 19th-century adolescent who happens to be a mathematical genius.

Petsinis is either very brave or very foolhardy to have made the attempt, and if the effort has been only partly successful, that hardly comes as a surprise. To me what is most convincing are the frequent references early on to Pindar, Catullus, and Hugo, not to mention Archimedes, Euclid, and Pythagoras—classical literature and mathematics that any child of Galois's generation would have been immersed in. What is sometimes believable as well is Galois's black-and-white outlook on things. During the first part of the novel, which takes place at the lycée, Evariste is only 15, and a black-and-white worldview comes, as they say, with the territory.

But here the decision to tell the story in the first person does not serve. Galois's writings are hardly voluminous and he was certainly not a happy young man—the word "detest" leaps off his pages. Petsinis's Galois detests everyone and everything—he says so often. Without any other substantive characters in the book to balance such pronouncements, Galois's story quickly becomes a one-note performance. There is little sign of the great affection for his parents and relatives that Paul Dupuy, Galois's original biographer, describes and that is evident in his letters. To be sure, a constant danger of a first-person narrative is that the subsidiary characters will fade into the background. That is precisely what happens here. Evariste's mother, who was responsible for his early education, was by all accounts an intelligent, lively woman even into old age, and one who saw religion

in the light of ethics. Petsinis has portrayed her as something of a religious fanatic. "Your father has turned from God, she glares. Paris! The new Babylon! The haunt of the Evil One! The source of atheism! I fear the Apocalypse is at hand! The signs are there: crime, debauchery, chaos! Don't go back, Evariste. Stay here and help me lead your father back to God." I am sure Petsinis chose this portrayal to prepare the way for her break with Evariste, which did take place when he was about 20. But it seems so unnecessary, and the dialogue ludicrous, when her son's behavior is itself enough of an explanation.

By the same token, Galois's father, the liberal mayor of Bourg-la-Reine, is a mere cipher. Women other than Galois's mother, to the extent that they figure at all in the book, are mostly prostitutes standing in doorways (Galois detests the thought of sex; only mathematics is pure), and the July revolution consists mostly of crowds chanting the usual slogans: "Freedom of the press!" "Liberté, égalité . . . ." Somewhat strangely, Galois himself appears as a reluctant revolutionary who turns from mathematics to politics only after his father commits suicide in the wake of a Jesuit plot against him. True, the choice allows for the character's evolution, but it does contradict everything anyone has written about Galois—and the passion evident in his own writings.

Which leads to the second hurdle Petsinis faces: is this a 19th-century Galois? Partly. As I have said, the milieu Petsinis has created strikes one as credible. On the other hand, the sense of verisimilitude is occasionally shaken by some of Galois's internal monologues, which sound surprisingly modern:

> If I focus on the point, the line proves an illusion. Astonishing that something so intangible should be the basis of all geometry! In a flash, I see the indivisible point as the seed of creation. Perhaps the universe exploded from the primal point. Perhaps God is the primal point. Perhaps the soul is nothing more than a point.

Similar references to the fate of stars and to the nature of space and time do sometimes make Galois seem more like a 20th-century astrophysicist than a 19th-century mathematician. The problem is again exacerbated by the first-person narrative. We are able to see Galois only as he sees himself, not as others see him. In this instance the effect is not to bring Galois alive. Here is Petsinis's Galois describing the famous Preface to his work he wrote while in prison:

> I also managed to write a four-page preface to the book that would contain my collected work . . . I denounced patronage and attacked the Academy for losing my manuscripts . . . . This was followed by a summary of the two papers I had reworked. . . .
>
> I then went on to denounce Poisson and the examiners at the Polytechnique. Even though I had reason to believe the scientific fraternity would greet my work with a condescending smile, I persisted in trying to have my work published. . . .
>
> Finally, I tackled the question of why readers found my work so difficult, even incomprehensible, and concluded it was due to my inclination to dispense with formalisms and calculations.

Here is some of the original:

> I tell no one that I owe anything of value in my work to his advice or encouragement. I do not say so because it would be a lie. If I addressed

anything to the important men of science . . . I swear it would not be thanks. I owe to important men the fact that the first of these pages is appearing so late. I owe to other important men the fact that the whole thing was written in prison, a place, you will agree, hardly suited for meditation, and where I have been dumbfounded at my own listlessness in keeping my mouth shut at my stupid, spiteful critics . . . . The whys and wherefores of my stay in prison have nothing to do with the subject at hand, but I must tell you how manuscripts go astray in the portfolios of the members of the Institute, although I cannot in truth conceive of such carelessness on the part of those who already have the death of Abel on their consciences.

Is there any question which is the living Galois?

One is left feeling that a more effective strategy might have been to surround Galois by a group of third-persons trying to make out this character, refractory by Petsinis's own admission. Be that as it may, the sharpest issue raised by *The French Mathematician* centers on the portrayal of a mathematician. Art is of course enriched when it can find inspiration in science and mathematics. But is what we have here a convincing portrait? As a mere theoretical physicist, I have no special expertise. Nevertheless, I find it peculiar that any mathematician would be engaging in mathematical metaphors while dying, as Galois does:

I embraced that fatal sphere with my whole body. Dreams, memories, even the mathematics I had cherished and set down in my last will and testament —all receded. I am reduced to a singular point; in an instant I am transformed to i.

i = an imaginary being

But Petsinis's Galois compares and contrasts everything with mathematics, even his true love: "Our fingertips touch. I summon all my courage to look into her eyes. There I am, circumscribed by her pupils. And in that instant π reveals its perfect proportion and is reduced to a chaos of digits, the Republic is created and destroyed, I am extinguished and reborn."

Well, perhaps I've never known a mathematician of Galois's caliber, but I find this pretty laughable. And this brings me to the main point. What *The French Mathematician* shares with its predecessors is the intention to portray a mathematician as a thing apart. It is an intention that Hollywood would appreciate; its typical scientists are direct descendants of Frankenstein. Strange that both the scientific and nonscientific communities seem bent on keeping scientists and nonscientists as distant from each other as possible. When Andrew Wiles announced his proof of Fermat's last theorem, the *New York Times* portrayed him as a man who had locked himself in an attic for seven years. Having been a close friend of Wiles during much of that time, I can state categorically that he is a man of broad literary interests who was an avid film-goer and was not above going out for a beer on Saturday evenings; he could also find work as a romance counselor.

One can't help suspect that there is some deep-seated need on the part of both the scientific and the nonscientific communities to maintain their separation. The result is not only a great deal of misunderstanding about what science is, but also a real antipathy between scientists and others—especially between scientists and artists. The situation is analogous to existing divisions in the publishing domain: literature is divided into genres, and each genre must have standard devices.

(Suspense novels must contain the prerequisite amounts of sex, violence, and endings that result in an explosion, narrowly averted.) Editors tell you this. Any novel that doesn't conform to these conventions is deemed unbelievable. And so the reality of the genre has replaced the reality of the real world.

In some respects the relationship between the sciences and the humanities long ago fell into the pattern of genre fiction. This is unfortunate and does not adequately reflect the reality of the world. In fact, mathematics and science have influenced art more, perhaps far more, than is usually acknowledged. In the late 19th century, speculation on the meaning of the "fourth dimension" was extremely popular and influenced the work of futurist and suprematist artists, who in turn influenced world architecture through Bauhaus. Einstein's relativity prompted artists and musicians of the 1920s to speculate on the nature of space and time, which resulted in the machine esthetic. Marcel Duchamp's famous "Large Glass" in Philadelphia was actually based on his musings about physics. Some historians argue that Girard Desargues invented projective geometry as a result of concern with perspective in art.

And so on. That is the way civilization is created, not by streams running each in its own course, but by streams coursing together. I can't help think that it is long past time on the part of both writers and scientists to emphasize their commonality of experience rather than their separateness of existence.

REFERENCES

1. Eric Temple Bell, *Men of Mathematics*, Simon and Schuster, New York, 1937.
2. André Dalmas, *Evariste Galois, Révolutionnaire et Géomètre*, Fasquelle, Paris, 1956.
3. Leopold Infeld, *Whom the Gods Love: The Story of Evariste Galois*, Whittlesey House, New York, 1948.
4. Tony Rothman, Genius and biographers: the fictionalization of Evariste Galois, this MONTHLY **89** (1982) 84–106.
5. Tony Rothman, *Science à la Mode: Physical Fashions and Fictions*, Princeton University Press, 1989. Chapter 6 is a revised version of [**4**] containing new material; it is also available at `http://titan.iwu.edu/~trothman`.

Illinois Wesleyan University, Bloomington IL 61702
trothman@titan.iwu.edu

Social Constructivism as a Philosophy of Mathematics. By Paul Ernest. State University of New York Press, 1998, xiv + 315 pp., \$19.95 softcover, \$59.50 hardcover.
What Is Mathematics, Really? By Reuben Hersh. Oxford University Press, 1997, xxiv + 343 pp., \$35.00.

Reviewed by **Bonnie Gold**

In the early years of this century, Platonism (by which I mean the belief that mathematics is the science of certain mind-independent, non-physical objects with determinate properties) was dethroned as the dominant philosophy of mathematics. Since then, there's been a struggle to replace it with an alternative that avoids the philosophical problems of Platonism while accurately reflecting the working mathematician's daily experiences of doing mathematical research.

None of Platonism's immediate successors—logicism, formalism, intuitionism—has proved satisfactory. The first two fail to account for the role of the mathematician in the establishment of mathematical knowledge, as if mathematical knowledge were possible without any mathematicians. They also don't allow for the development of our knowledge of mathematics over time. The third, intuitionism, is unpopular because it rejects large parts of mathematics. As the philosophy of science started studying how scientific knowledge develops and the reasons for accepting new scientific theories, Lakatos and others began similar inquiries about mathematics. In the last 25 years, new candidates for philosophies of mathematics have become popular, including fictionalism, conventionalism, structuralism, and social constructivism.

In the books under review, both Paul Ernest and Reuben Hersh propose versions of social constructivism, which has been gaining adherents recently. However, their writing styles and viewpoints are completely different. Although each author speaks warmly of the other, they represent opposite extremes of the school. Mathematicians will almost universally find Hersh's version palatable and Ernest's unpleasant to read and at odds with actual mathematical practice.

Part of the problem with Ernest's book is really the fault of mathematicians, especially teachers of logic. Philosophy students often take a required mathematics course without really understanding it—they never internalize DeMorgan's laws (the negation of "p and q" is "not p *or* not q"), and they don't appreciate the importance of correct hypotheses in theorems—but they work so hard that we give them a passing grade. Alas, some of them go on to graduate school and beyond, and start writing books about the philosophy of mathematics that make us shudder with embarrassment as they betray their total lack of understanding of mathematics.

Ernest is a philosopher who thinks he knows about mathematics because he's taken a few courses in mathematical logic. He hasn't understood them. He bases a part of his philosophical position on an incorrect statement of the Craig Interpolation Lemma. The lemma says that if one has two formulas A and B, possibly involving different symbols, and a proof that $A \to B$, then there is a formula X involving only symbols that occur in both A and B such that there are proofs that $A \to X$ and $X \to B$. That is, if one formula implies another, then there is an interpolant in a language that they have *in common*. Ernest first states the lemma incorrectly (p. 204, footnote 13), saying that X "*includes* the mathematical concepts occurring in both A and B"—that is, it might be in a larger language! Then, he uses this bizarre misstatement of the theorem to claim that "no step from A to B in a proof is above further analysis, and there are no ultimate basic proof steps into which a published mathematical theorem can be analyzed." Yet, once one has interpolated an X that is in the common language, there's nothing further to be done! Certainly one can trivially add X arbitrarily often as an interpolant: $A \to X$, $X \to X$, $X \to X$, and $X \to B$; but this adds nothing, whereas the original act of interpolation in some sense gets at what A and B have in common that *makes* A imply B. After that, there is nothing *further* to analyze.

This confusion is not a central point in Ernest's argument (although he does refer to it twice, using it to claim that it's not possible, even in principle, to reduce all proofs to a standard format), but it is typical of the lack of understanding of mathematics found throughout the book. He gives few concrete mathematical examples of what he is talking about, and when he does, frequently they are either incorrect or a misinterpretation of the mathematical result.

The audience for the book is clearly professional philosophers of mathematics, not mathematicians. Since the book is full of terms such as "reification" and "hermeneutic" and references to philosophers such as Gadamer, Bakhtin, and Collingwood, mathematicians will find it extremely tough slogging unless they have a good knowledge of philosophy and have closely followed the writings in philosophy of mathematics over the last 30 years.

The philosophical point of view Ernest puts forth is that mathematics is simply whatever the community of mathematicians chooses to call "mathematics", and mathematical truths are simply what we decide to baptize as truths. If tomorrow we decide that $\mathbf{Z}_6$ has a subgroup of order 5, then it will, and that will be as "objectively" true as the fact, today, that it doesn't. Recognizing that he has to account for the apparent "objectivity" of mathematics, Ernest simply uses Orwell's Newspeak as a model and says that if a community agrees something is true, that's "objectivity." He accounts for the universal agreement on the facts of mathematics by the observation that we bully our students in grade school to accept such "conventions" as "$2 + 2 = 4$," so that by the time they get to college they view it as a law of nature.

The basis of Ernest's views is what he sees as extensions of the work of Wittgenstein and Lakatos. From Wittgenstein he takes the view that mathematics is a verbal game, played by rules. The rules are looked after by the community of mathematicians, and we accept new members into our community when they show that they can follow those rules. What the rules are, he declines to specify, although they include "proof," which he views as a kind of conversation (again, unspecified, but varying over time) to "warrant" mathematics (a philosophical term roughly meaning to give a basis for something to count as an object of knowledge). Proof is by no means the *only* rule of the game: there are rules for discovery, for writing or discussing mathematics, etc., but no details beyond general principles are given. There is nothing even conceivably fixed in any of these rules —rather, Ernest insists that NO text can have a unique meaning, but simply has the meaning the community chooses to give it at present. As has become popular among philosophers of mathematics, he cites the Lowenheim-Skolem Theorem in support of this view, although this theorem is about first-order logic only, not all of mathematics.

From Lakatos, Ernest takes the view that the philosophy of mathematics must be considered from a historical perspective, and revolutions in mathematics are a regular part of mathematical practice. Ernest takes this to mean that no facts are permanently true; "facts" true today may become false tomorrow. This is simply false. There are changes in the meanings of some words and different levels of rigor over time, so our philosophical interpretations of the mathematics change. But the facts themselves simply don't change. Although other sciences and philosophical theories change their "facts" frequently, 2 + 2 remains 4.

Hersh's book is an attempt to set forth in greater detail the philosophy mentioned cursorily in his books written with Philip J. Davis, *The Mathematical Experience* and *Descartes' Dream*. These books have done a substantial service to the mathematical community, and to the world at large, by attempting to bridge the gap between mathematicians and everyone else. There is far too little of this kind of expository writing by mathematicians. Hersh targets the same wide audience in this new book, but in this case he serves no one well by the ambiguity of audience. There are too many references to specific mathematical facts for anyone without an undergraduate degree in mathematics fully to understand the book

(despite a final section that briefly explains various mathematical topics). On the other hand, the lack of specific references for his myriad quotes and paraphrasings makes it a Herculean task for the mathematician or philosopher to examine the contexts of the quotes.

The title "What is Mathematics, *Really*" is in response to "What is Mathematics" by Courant and Robbins **[1]**, which "answered" the question by providing some very nice examples of mathematics, but which never summed up these examples in a clear, concise statement. Hersh's book, an attempt to provide that statement, consists of three parts. The first part sets forth his philosophy of mathematics in a brief, well-written 90 pages. While I don't believe that this is *the* correct view of mathematics, Hersh makes the case well. He has the best account (pp. 61–62) I've seen of the role of intuition in mathematics: the various ways mathematicians use the word and its importance in both the development of new mathematics and decisions about the correctness of this new mathematics. It's worth getting the book simply to read this discussion. The second part is his particular take on the history of the philosophy of mathematics, in which he divides philosophers of mathematics into mainstream or humanist. I'm not sufficiently well-versed in this history to judge the accuracy of his division; the lack of detailed references is especially annoying in this part of the book. His classification of Brouwer with the traditionalists is particularly bizarre. Any reasonable understanding of intuitionism would place Brouwer as a forerunner of the social constructivist school: for intuitionists, mathematics is that which the community of mathematicians constructs; mathematical objects don't exist until constructed by mathematicians. The final part of the book begins with an extremely offensive classification of philosophers of mathematics into leftists and rightists, resulting in a body count of far more leftists on the humanist side and more rightists on the traditional side. (Of course, moving Brouwer to the correct side of the traditionalist/humanist controversy makes the count less one-sided.) I see it as a desperate argument to sway mathematicians (who mostly tend to be generous souls) toward his philosophy. This is followed by 65 pages of mathematical notes and comments, an attempt to make the various mathematical references through the body of the text accessible to the lay reader.

Thus, the main new contribution of this book is in its first 90 pages. Hersh begins by discussing the problems of Platonism. The traditional Platonist view is that "mathematical entities exist outside space and time, outside thought and matter, in an abstract realm independent of any consciousness, individual or social" (p. 9). The traditional philosophical difficulties with this view are (1) it requires a belief in some abstract, non-physical, non-psychological realm, which might have been fine when God was central to our world-view, but which is unattractive to modern intellectuals, and (2) even if such a realm exists, how do we, physical beings, have any contact with, or knowledge of, this realm? To the best of my knowledge, there haven't been any serious recent attempts by mathematicians to modify Platonism to meet those objections. This leaves the field open for philosophers to declare victory over Platonism, and to offer alternative philosophical descriptions of mathematics.

It's not clear that any modern mathematicians who view themselves as Platonists (or "realists") actually subscribe to Hersh's full statement. Most mathematicians are not particularly committed to where or what mathematical objects are, just as long as they do have objective properties. Therefore Hersh's view is attractive: mathematical objects are constructed by the community of mathematicians. Generally a new concept is suggested by one mathematician, but often the idea is

developed and modified over a period of time by the community until it settles down to have a fixed definition.

Mathematical objects, then, are neither mental nor physical; rather, they are social entities, in the same general category as monetary systems, or the Supreme Court (not the people, but the institution). So far, Hersh and Ernest are in rough agreement. For Hersh, however, once a mathematical object has been constructed by the community of mathematicians, it takes on a sort of life of its own. Its properties are no longer dependent on people, but are discovered; some properties, not apparent when we first define the object, can be difficult to discover. This is the point at which Hersh and Ernest part company. For Ernest, only the current rules of the mathematical game make x^2 an even function, and it could become odd at any time. For Hersh, once the function has been defined, mathematicians no longer control it.

Hersh's version has several very attractive features. It fits fairly well with mathematics as done by mathematicians. Our knowledge of mathematics develops over time, as well it should if mathematicians invent new mathematical objects or discover connections among those already invented. Mathematics is no longer infallible, but that's much more consistent with our actual experience than is the purported infallibility of traditional Platonism. After all, false proofs are often published, and mistakes are common when one works on new mathematics. Under Hersh's view, the mathematical community determines what constitutes a proof, and proof becomes the standard set by the community for acceptance of new mathematical knowledge. This describes actual mathematical practice far better than formalism's view that proofs are deductions in first-order logic, of which no human can comprehend any non-trivial examples. Further, there's a role for mathematics education: it brings new members into the community.

However, there are two important ways in which Hersh's social constructivism is inadequate as a philosophy of mathematics. The first is that it doesn't account well for the usefulness of mathematics in the world. Why should mathematics developed *before* any application was known turn out to be useful, and often in a variety of unrelated contexts? Certainly social constructivism can explain the parts of mathematics developed in response to some societal need. But the majority of applications, especially in this century, came from mathematics developed for the pure interest of the mathematical question—so why should it later be found to have anything to do with the real world?

The second, and, I think, the more serious problem with social constructivism is that it doesn't distinguish between the facts of mathematics (the function x^2 is even, the group $\mathbf{Z}_6$ has subgroups of order 1, 2, 3, and 6) and *our knowledge* of that mathematics. Plato's bizarre suggestions on recollection from past lives aside, it's clear that as children we are taught mathematics; the mathematical community's *knowledge* of mathematics *develops* over time; and it involves a communal effort. That social constructivist philosophies do recognize this development, and credit it, is a principal reason they are attractive. But this recognition is not an argument against the independence of mathematical objects from human society. Our knowledge of physics also develops over time. Nonetheless, the facts of physics exist before their discovery, and they are independent of errors the community of physicists makes or debates within that community. Furthermore, the concepts of physics—atoms, velocity, force, and so on—are developed gradually by the community of physicists. Yet physical objects either are or are not made up of atoms, and it's not the community of physicists that makes that true or false: it's the actual state of the world. That is, people develop and clarify concepts, but the *objects*

those concepts attempt to describe either are or are not present in the world. The same is true of the objects of mathematics. Symmetry properties of chemicals affect how those chemicals behave, and did so even before mathematicians discovered symmetry groups. Ropes didn't start hanging in catenaries only after mathematicians "invented" that curve.

Hersh consistently ignores this distinction between the facts of mathematics and our knowledge of those facts, and many of his statements become obviously false if one reads them with this distinction in mind. "From living experience we know two facts: Fact 1: Mathematical objects are created by humans..." (p. 16). In what way does our "creation" of $\mathbf{Z}_6$ differ from our creation of quarks? Clearly, we single out the concept as something worth applying to part of our experience, but that isn't *creating* the object. "Point 1 is that mathematics is a social-historic reality. This is not controversial" (p. 23). No, it's not controversial, just false. Our *knowledge* of mathematics is a social-historic reality, though, and *that* isn't controversial.

There are several other problems with Hersh's account of mathematics. "A realistic analysis of mathematical intuition should be a central goal of the philosophy of mathematics" (p. 62). Hersh asserts that our intuition of mathematical objects comes from our education, from doing problems and getting checked for correctness by our teachers. We check that we have the same representation of a concept by seeing if we give the same answers to questions about it. That is, it's a social activity. But this doesn't square with experiences such as that of Ramanujan, who developed his results in complete isolation. Certainly, without a community of mathematicians—and especially without Hardy—to recognize the importance of his work, it would have been lost to the world. But Ramanujan's intuition came from working with the mathematical objects themselves, not from the community. While Ramanujan's case is certainly the extreme, the history of mathematics has numerous other examples of mathematicians (Desargues and Abel come to mind) who were so far ahead of their time that there was no *community* developing the intuition behind their discoveries.

In the past, a requirement of a philosophy of mathematics has been that it account for the peculiar level of certainty we appear to have in mathematics. The three philosophical schools that developed around the turn of the century—logicism, intuitionism, and formalism—were the result of trying to regain the level of certainty for which mathematics was notorious before the discovery of non-Euclidean geometry, contradictions in set theory, and problems in the foundations of analysis. Hersh spends a lot of time trying to debunk the notion of "mathematical certainty" on the grounds that formal proofs don't give certainty, because nontrivial ones aren't surveyable, and whence does our certainty come, if not through formal proofs? Yet once the definitions are understood, *any* two mathematicians, no matter what their cultures, should come to the same conclusions. That is different even from other sciences, not to mention studies (e.g., economics, politics) of the "socio-historical objects" Hersh would place mathematics among. Even if proofs don't give absolute certainty, proofs are central to the establishment of a mathematical result. I'm happy to view proofs among the activities that concern human knowledge of mathematics, not the mathematics itself. But nothing in Hersh's account explains the special role of proof in mathematics—why it's so central for establishing the truth of mathematical facts. An adequate philosophy of mathematics must do a better job of incorporating the role of proof, beyond explaining it as a peculiar social custom.

I'm a mathematician. I work every day with such mathematical objects as the function x^2 and the group (or ring) $\mathbf{Z}_6$. I'm not really sure where or what these objects are. But I am sure that *nothing* the human community (mathematicians or otherwise) does will make x^2 into an odd function or make $\mathbf{Z}_6$ have a subgroup of order 5. And any philosophy of mathematics that says otherwise must simply be rejected.

What is needed is an account of mathematical objects, and facts of mathematics, and our knowledge of these facts, that parallels the account of physical objects and facts of physics and our knowledge of them. This may be roughly what Gödel meant when he wrote, "Despite their remoteness from sense experience, we do have something like a perception also of the objects of set theory, as is seen from the fact that the axioms force themselves upon us as being true.... This, too, may represent an aspect of objective reality" [**2**]. There's no reason to believe, as Hersh asserts, that Gödel believed this perception true only of sets and not of other mathematical objects.

There is one alternative philosophy of mathematics that rivals social constructivism in growing popularity, but that Hersh touches on only briefly and trivially dismisses. It is the closest to a current attempt to account for mathematics in a Platonist manner while meeting the philosophical objections to older Platonist accounts. This is the view of mathematics as "the science of pattern." While many mathematicians have supported this view (Lynn Steen and Peter Hilton among them), I'm unaware of any attempt on the level of the two books under review to present this view carefully and in detail. Hersh's objection that mathematics doesn't study *every* kind of pattern is trivially correct. That is why this view needs further exploration. However, the view that mathematics is the science of *certain kinds* of patterns allows mathematics to be independent of society and yet accounts for the ability of physical beings to contact objects in the world of mathematics.

One thing human beings do extremely well is to observe patterns. We're far superior to computers in this ability. With great difficulty we can program computers to recognize very simple patterns, but human beings recognize some patterns when we are born and very quickly learn to recognize and work with many kinds of patterns. Furthermore, patterns partake of both the physical and the non-physical. In fact, we can see our ability to classify *anything* as a recognition of patterns. One collection of atoms, of leaves and branches in certain patterns, is a tree. We recognize the general pattern by giving it this collective name. Another pattern is a table. Some patterns are man-made, others are out there in the world, others are abstract, but our minds are what give them a collective name. To the extent that we say that trees are objective and not dependent on the human mind, we can start attributing that same objectivity to the patterns mathematicians study. It's certainly not the case that all patterns are mathematics. But at least somewhere in that region there seems a place to carve out the realm of mathematics—neither physical, mental, nor social, but certainly associated with the world, independent of us, and accessible to human beings.

Such a view does a better job of accounting for the applicability of mathematics, for many of our patterns come from the physical world. That our knowledge of mathematics develops over time becomes no more surprising than that our knowledge of physics develops over time. That different cultures have been especially hospitable to the discovery of certain parts of our mathematical knowledge is almost inevitable, as the patterns that a culture surrounds itself with are particular to it—and so our mathematical *knowledge* is very much a socio-cultural

artifact. How proof helps guarantee mathematical truth remains to be explored, but it's reasonable that a link can be found in the connection between patterns in the world and mathematicians looking for them.

Although in the end I don't believe Hersh has yet shown us *what is mathematics, really*, he has made an important contribution to the discussion. Any acceptable philosophy of mathematics must be consistent with actual practice of mathematicians—that we make errors, that our proofs are *not* exercises in formal logic, that our knowledge changes over time. Whatever we finally decide mathematics is, it is still discovered by humans; what is discovered may depend on social or cultural factors; and the discovering, teaching, and sharing of our knowledge of mathematics remains something to be shared by all, both for the benefit of the growth of that knowledge and for the human race's ability to rise above petty fraternal feuds.

REFERENCES

1. Richard Courant and Herbert Robbins, *What Is Mathematics*? Oxford University Press, fourth edition, 1948.
2. Kurt Gödel, "What is Cantor's Continuum Problem?" reprinted in *Philosophy of Mathematics: Selected Readings*, second edition, Paul Benacerraf and Hilary Putnam, eds., Cambridge University Press, 1983, pp. 483–484.

Monmouth University, West Long Branch, NJ 07764
bgold@mondec.monmouth.edu

Today Devin catches me at it.
"Mommy, what're you trying to do?"
"Oh," I say, "well, these lines.
I'm trying to fix these lines."
And then I explain triangles.
And then I explain transitive.
"Sometimes it can't be done," I tell him, "and other times it can.
I'm trying to figure out when it can."
"I get it," he says. "I get it, Mommy."
And later he catches me at it again.
"*That* one *worked*, right?"

'Cause maybe, if that one worked, we can go play Parchesi.
Or cards. Or ice cream. Or hanging out.
Or at least Mommy won't
keep staring at those lines.

Contributed by Marion Cohen, Drexel University, Philadelphia, PA

TELEGRAPHIC REVIEWS

Edited by **Arnold Ostebee**
with the assistance of the Mathematics Departments of Carleton, Macalester, and St. Olaf Colleges

Telegraphic Reviews are designed to alert readers in a timely manner to new books appropriate to mathematics teaching and research. Special codes classify reviews by subject area and appropriate use:

T : Textbook	*P : Professional Reading*	*1–4: Semester*
C : Computer Software	*L : Undergraduate Library*	*** : Special Emphasis*
S : Supplementary Reading	*13: Grade Level*	*?? : Questionable*

Readers are advised that price information is subject to change. Selected books receive a second, more extensive review in the *Monthly*.

Books submitted for review should be sent to *Book Reviews Editor, American Mathematical Monthly, St. Olaf College, 1520 St. Olaf Avenue, Northfield, MN 55057-1098.*

General, L. *The Mathematical Tourist: New and Updated Snapshots of Modern Mathematics.* Ivars Peterson. WH Freeman, 1998, xviii + 266 pp, $14.95 (P). [ISBN 0-7167-3250-5] Augments and updates the 1988 *First Edition* (TR, October 1988); new material treats large primes, quantum computing, cellular automata, the nature of proof, Wiles's proof of Fermat's theorem, and more. Rich with figures and illustrations, including 16 in striking color. Includes about 40 short, readable essays, all accessible to nonspecialist (but careful) readers. PZ

General, S(16–17), L. *Berkeley Problems in Mathematics.* Paulo Ney de Souza, Jorge-Nuno Silva. Problem Books in Math. Springer-Verlag, 1998, xiv + 443 pp, $59.95. [ISBN 0-387-94934-8] Problems and solutions in real and complex analysis, calculus, differential equations, linear and abstract algebra from 20 years of Berkeley preliminary exams. Good resource for graduate students as well as undergraduates. JD

General, S?(13). *The Most Beautiful Mathematical Formulas.* Lionel Salem, Frédéric Testard, Coralie Salem. Transl: James D. Wuest. Wiley, 1992, xiii + 141 pp, $24.95. [ISBN 0-471-55276-3] A trove of forty-nine formulas (elementary geometry, algebra, trigonometry, number theory) deplorably hyped-up with phony story problems. LCL

Reference, P. *The Wonderful World of Mathematics: A Critically Annotated List of Children's Books in Mathematics, Second Edition.* Diane Thiessen, Margaret Matthias, Jacquelin Smith. NCTM, 1998, xi + 355 pp, $17.95 (P). [ISBN 0-87353-439-5] Includes books published since the 1992 edition (TR, May 1994); omits most out-of-print titles. More than 60% of titles are new. New subsection on quilting. Great resource for parents, teachers, teacher educators. KES

Recreational Mathematics, S, P, L***.** *Dissections: Plane & Fancy.* Greg N. Frederickson. Cambridge Univ Pr, 1997, xi + 310 pp, $34.95. [ISBN 0-521-57197-9] A beautiful book that entices, entertains, fascinates, and instructs. Collects, organizes, and presents 2000+ years of discovery alongside exciting new contributions. Complete, thorough, fun to read; this will be a classic. Only prerequisite is basic knowledge of high school geometry. LCL

Education, T(15–17), S*, P, L. *Glimpses of Algebra and Geometry.* Gabor Toth. Grad. Texts in Math. Springer-Verlag, 1998, xviii + 308 pp, $39.95. [ISBN 0-387-98213-2] For a "bridge course" among undergraduate and graduate studies. Focuses on connections and interactions between number theory, classical geometry, and modern algebra. Includes web addresses for additional information, interactive graphics, and animations. LCL

History, P, L. *Cauchy and the Creation of Complex Function Theory.* Frank Smithies. Cambridge Univ Pr, 1997, 216 pp, $59.95. [ISBN 0-521-59278-X] Careful, detailed analysis of Cauchy's contributions to complex analysis during the period 1814–1831 including work on the Cauchy–Riemann equations, Cauchy's Theorem, residue theory, contour integration,

and Rouche's Theorem. Scholarly and well-documented. Not light reading. BH

History, P, L. *Mathematics and Mathematicians: Mathematics in Sweden before 1950.* Lars Gårding. History of Math., V. 13. AMS, 1998, xiii + 288 pp, $75. [ISBN 0-8128-0612-2] Comprehensive description beginning in the 1700's. Clear exposition of the many mathematical contributions of the Swedes as well as glimpses into their personal lives. Includes a short biography of one of the most influential Swedish mathematicians, Gösta Mittag–Leffler, who founded Acta Mathematica and brought Sonya Kovalevski to Sweden. BH

History, P. *Collected Papers of Paulo Ribenboim, Volumes 1–7.* Paulo Ribenboim. Papers in Pure & Appl. Math., V. 104. Queen's Univ, 1997, [ISBN 0-88911-735-7] set, (P). *Volume 1*, xlviii + 506 pp, [ISBN 0-88911-783-7]; *Volume 2*, ii + 532 pp, [ISBN 0-88911-785-3]; *Volume 3*, ii + 550 pp, [ISBN 0-88911-787-X]; *Volume 4*, ii + 580 pp, [ISBN 0-88911-789-6]; *Volume 5*, ii + 573 pp, [ISBN 0-88911-791-8]; *Volume 6*, xviii + 581 pp, [ISBN 0-88911-793-4]; *Volume 7*, ii + 570 pp. [ISBN 0-88911-795-0]

Logic, C, P. *Consequences of the Axiom of Choice.* Paul Howard, Jean E. Rubin. Math. Surv. & Mono., V. 59. AMS, 1998, vii + 432 pp, $89, with disk. [ISBN 0-8218-0977-6] Comprehensive list of statements proved using the Axiom of Choice. Includes proofs not readily available in the literature; gives references for others and for relationships between consequences. Describes models of set theory. Accompanying software provides access to information on a single consequence or a pair of consequences. KES

Logic, T(15–16: 2), L. *The Incompleteness Phenomenon: A New Course in Mathematical Logic.* Martin Goldstern, Haim Judah. AK Peters, 1998, xiii + 247 pp, $39 (P). [ISBN 1-56881-093-8] Paperback edition (TR, October 1996).

Combinatorics, P. *Steiner Minimal Trees.* Dietmar Cieslik. Nonconvex Optimiz. & Its Applic., V. 23. Kluwer Academic, 1998, xi + 319 pp, $140. [ISBN 0-7923-4983-0] Examines Steiner's Problem (and some of its relatives) in the setting of arbitrary finite-dimensional Banach spaces.

Linear Algebra, T(14), L. *Linear Algebra with Applications, Fifth Edition.* Steven J. Leon. Prentice Hall, 1998, xiv + 491 pp. [ISBN 0-13-849308-1] Follows guidelines of the NSF-sponsored Linear Algebra Curriculum Study Group. Applications scattered throughout; MATLAB exercises in every chapter. Includes chapter on numerical linear algebra. (*Third Edition*, TR, February 1991.) JD

Ring Theory, S(15–16), L. *Exercises in Basic Ring Theory.* Grigore Călugăreanu, Peter Hamburg. Texts in the Math. Sci., V. 20. Kluwer Academic, 1998, xiv + 198 pp, $90. [ISBN 0-7923-4918-0] Problems and solutions. Topics include homomorphisms, division rings, Artinian and Noetherian rings, socle and radical, and polynomial rings. Avoids modules and field theory. JD

Algebra, P. *Recent Progress in Algebra.* Eds: Sang Geun Hahn, Hyo Chul Myung, Efim Zelmanov. Contemp. Math., V. 224. AMS, 1999, ix + 243 pp, $55 (P). [ISBN 0-8218-0972-5] Selected papers from a 1997 conference at KAIST, Taejon, South Korea.

Calculus, T*(13: 3). *Calculus: Concepts and Contexts.* James Stewart. Brooks/Cole, 1998, xx + 1131 pp, $102.95. [ISBN 0-534-34330-9] Excellent synthesis of traditional and reform approaches to calculus instruction. Stresses conceptual understanding through geometric, numeric, and algebraic approaches. Retains a modest and appropriate amount of rigor. Frequently uses real data in numerical exercises. Includes several interesting projects. RL

Real Analysis, P, L. *Theory of Differentiation: A Unified Theory of Differentiation Via New Derivate Theorems and New Derivatives.* Krishna M. Garg. Canadian Math. Soc. Ser. of Mono. & Adv. Texts, V. 24. Wiley, 1998, xv + 525 pp, $125. [ISBN 0-471-25387-1] Comprehensive, detailed account of differentiation of real-valued functions. Includes discussion of outstanding problems. For experts. KS

Differential Equations, P. *Boundary Value Problems and Symplectic Algebra for Ordinary Differential and Quasi-Differential Operators.* W. Norrie Everitt, Lawrence Markus. Math. Surv. & Mono., V. 61. AMS, 1999, xii + 187 pp, $49. [ISBN 0-8218-1080-4]

Differential Equations, P. *Basic Topological Structures of Ordinary Differential Equations.* V.V. Filippov. Math. & Its Applic., V. 432. Kluwer Academic, 1998, xiv + 516 pp, $225. [ISBN 0-7923-4951-2]

Dynamical Systems, P. *Dynamical Systems Approach to Turbulence.* Tomas Bohr, *et al.* Nonlinear Sci. Ser., V. 8. Cambridge Univ Pr, 1998, xx + 350 pp, $85. [ISBN 0-521-47514-7]

Functional Analysis, T(18), S(16–18), P, L. *An Introduction to Banach Space Theory.* Robert E. Megginson. Grad. Texts in Math., V. 183.

Springer-Verlag, 1998, xix + 596 pp, $64.95. [ISBN 0-387-98431-3] First chapter could be called "Introduction to Banach Spaces." Four more chapters: weak and weak* topologies, linear operators, Schauder bases, rotundity and smoothness. Author has paid exceptional attention to detail. Over 450 exercises, lengthy bibliography, historical notes, and citations to original sources. An appendix suggests changes for an undergraduate course. KS

Functional Analysis, P. *Analytic Functionals on the Sphere.* Mitsuo Morimoto. Transl. of Math. Mono., V. 178. AMS, 1998, xi + 160 pp, $65. [ISBN 0-8218-0585-1]

Analysis, P. *The Gibbs Phenomenon in Fourier Analysis, Splines and Wavelet Approximations.* Abdul J. Jerri. Math. & Its Applic., V. 446. Kluwer Academic, 1998, xxvii + 336 pp, $162. [ISBN 0-7923-5109-6]

Analysis, P. *Applied Analysis.* Eds: J. Robert Dorroh, *et al.* Contemp. Math., V. 221. AMS, 1999, ix + 284 pp, $59 (P). [ISBN 0-8218-0673-4] Papers from special sessions at the 1996 Southeastern Regional Meeting of the AMS held in Baton Rouge, Louisiana.

Analysis, P. *Existence Theory for Nonlinear Integral and Integrodifferential Equations.* Donal O'Regan, Maria Meehan. Math. & Its Applic., V. 445. Kluwer Academic, 1998, ix + 218 pp, $102. [ISBN 0-7923-5089-8] 12 surveys of recent results in Fredholm and Volterra integral and integrodifferential equations, resonant and nonresonant problems, integral inclusions, stochastic equations, and periodic problems.

Analysis, P. *Proceedings of the St. Petersburg Mathematical Society, Volume IV.* Ed: O.A. Ladyzhenskaya. AMS Transl., Ser. 2, V. 188. AMS, 1999, vii + 250 pp, $115. [ISBN 0-8218-0613-0] 11 papers on topics in analysis, probability, and applications.

Algebraic Geometry, T(18), P. *Moduli of Curves.* Joe Harris, Ian Morrison. Grad. Texts in Math., V. 187. Springer-Verlag, 1998, xiii + 366 pp, $59. [ISBN 0-387-98438-0] A guide to algebraic curves and how they vary in families. Emphasizes techniques and applications rather than reference material. Basic background in algebraic geometry necessary; more would be helpful. JD

Algebraic Geometry, P. *Representation Theories and Algebraic Geometry.* Eds: A. Broer. NATO ASI Ser. C, V. 514. Kluwer Academic, 1998, xxii + 443 pp, $205. [ISBN 0-7923-5193-2] Proceedings of a 1997 NATO Advanced Study Institute at the Université de Montréal.

Algebraic Geometry, P. *Vector Bundles and Their Applications.* Glenys Luke, Alexander S. Mishchenko. Math. & Its Applic., V. 447. Kluwer Academic, 1998, viii + 254 pp, $130. [ISBN 0-7923-5154-1]

Geometry, P. *Hypergeometric Functions, My Love: Modular Interpretations of Configuration Spaces.* Masaaki Yoshida. Aspects of Math., V. E32. Friedr. Vieweg & Sohn, 1997, xvi + 292 pp, $64. [ISBN 3-528-06925-2] Exuberant account of the modular interpretation of the configuration space of six lines on the projective plane. DB

Topology, P. *Tame Topology and O-minimal Structures.* Lou van den Dries. London Math. Soc. Lect. Note Ser., V. 248. Cambridge Univ Pr, 1998, x + 180 pp, $39.95 (P). [ISBN 0-521-59838-9] Self-contained treatment of *O*-minimal structures from geometric and topological viewpoints. Assumes only basics of algebra, topology, analysis. Of interest to model-theorists, geometers, and topologists. JD

Optimization, P. *Nonsmooth Approach to Optimization Problems with Equilibrium Constraints: Theory, Applications and Numerical Results.* Jiři Outrata, Michal Kočvara, Jochem Zowe. Nonconvex Optimiz. & Its Applic., V. 28. Kluwer Academic, 1998, xxi + 273 pp, $129. [ISBN 0-7923-5170-3]

Optimization, P. *Generalized Convexity, Generalized Monotonicity: Recent Results.* Eds: Jean-Pierre Crouzeix, Juan-Enrique Martinez-Legaz, Michel Volle. Nonconvex Optimiz. & Its Applic., V. 27. Kluwer Academic, 1998, xv + 467 pp, $208. [ISBN 0-7923-5088-X] 23 lectures from the Fifth Symposium on Generalized Convexity held in 1996 at CIRM, Luminy, France. Papers organized into four sections: Generalized Convexity; Generalized Monotonicity; Optimality Conditions and Duality; Vectorial Optimization. Each section contains at least one tutorial.

Elementary Statistics, T(1), C.** *Workshop Statistics: Discovery with Data and Minitab.* Allan J. Rossman, Beth L. Chance. Springer-Verlag, 1998, xxviii + 486 pp, $39.95 (P). [ISBN 0-387-98411-9] New version of *Workshop Statistics: Discovery with Data* (Springer-Verlag, 1996), the essential resource for activities-based statistics instruction. New version includes Minitab commands and macros, updated data sets. Extensive and helpful curricular support (e.g., data sets, Minitab worksheets) available on the internet. RL

Mathematical Statistics, T(16–17). *Bayesian Statistics: An Introduction, Second Edition.* Peter M. Lee. Wiley, 1997, xii + 344 pp,

$39.95 (P). [ISBN 0-471-19481-6] Expands *First Edition* by adding two chapters and increasing the number of exercises considerably. Solutions to exercises available on the web. HS

Statistical Methods, T(16: 1), C. *Statistical Case Studies: A Collaboration Between Academe and Industry.* Roxy Peck, Larry D. Haugh, Arnold Goodman. ASA–SIAM Ser. on Stat. & Appl. Prob. SIAM, 1998, xxxi + 282 pp, $26 (P), with disks. [ISBN 0-89871-413-3] 20 case studies using data sets from business, industry, or government. Data sets have not been simplified for classroom use. Cases are ordered by level of sophistication; most are at an undergraduate level. No exercises. HS

Statistical Methods, S(16). *An Introduction to Statistical Modelling.* Wojtek J. Krzanowski. Oxford Univ Pr, 1998, x + 252 pp, $19.99 (P). [ISBN 0-340-69185-9] Reference book with an applied slant. Covers core issues of classical statistical modeling. Focus is on the statistical aspects; only the most essential mathematical justifications are given. HS

Statistical Methods, T(17: 1), P, L. *Nonresponse in Household Interview Surveys.* Robert M. Groves, Mick P. Couper. Ser. in Prob. & Stat. Wiley, 1998, xiii + 344 pp, $79.75. [ISBN 0-471-18245-1] Discusses statistical impact of nonresponse on survey statistics, survey design features that might affect participation, the nature of interviewer-householder interaction producing the participation, and post-survey adjustments to correct for nonresponse. Assumes an initial undergraduate survey methods course. No exercises. KB

Statistical Methods, T(17–18, 1, 2), P, L. *Regression Analysis of Count Data.* A. Colin Cameron, Pravin K. Trivedi. Econometric Soc. Mono. Cambridge Univ Pr, 1998, xvii + 411 pp, $64.95; $24.95 (P). [ISBN 0-521-63201-3; 0-521-63567-5] An integrative survey of literature on count data regressions. Comprehensive and up-to-date. Makes sophisticated methods accessible to practitioners of different backgrounds. Emphasizes issues arising in econometric applications. KB

Statistical Methods, T(17: 1), P. *Applied Categorical Data Analysis.* Chap T. Le. Ser. in Prob. & Stat. Texts & Ref. Sec. Wiley, 1998, xiii + 287 pp, $64.95 (P). [ISBN 0-471-24060-5] For students and research workers in biomedical fields. Application oriented; mathematics kept to a minimum. Many real-life examples and computer program samples. HS

Statistical Methods, T(13: 1). *Statistical Quality Control: Strategies and Tools for Continual Improvement.* Johannes Ledolter, Claude W. Burrill. Wiley, 1999, x + 526 pp, $86.95. [ISBN 0-471-18378-4] Thorough coverage, with emphasis on understanding concepts and practical use. Covers nonstatistical problem solving tools and design of experiments for process improvement including Taguchi methods. Large collection of exercises and projects. Requires no statistical knowledge. KB

Applications (Quantum Theory), P. *Symmetries in Science X.* Eds: Bruno Gruber, Michael Ramek. Plenum Pr, 1998, ix + 454 pp, $139.50. [ISBN 0-306-45908-6] Proceedings of a 1997 symposium held at the Collegium Mehrerau in Bregenz, Austria.

Applications (Systems Theory), P. *Time-Varying Systems and Computations.* Patrick Dewilde, Alle-Jan van der Veen. Kluwer Academic, 1998, xiii + 459 pp, $122. [ISBN 0-7923-8189-0]

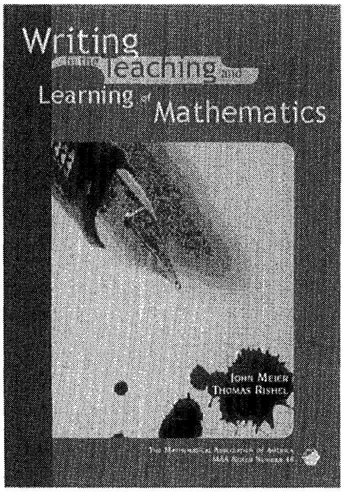
Applications (Systems Theory), T(16–17). *Mathematical Control Theory: Deterministic Finite Dimensional Systems, Second Edition.* Eduardo D. Sontag. Texts in Appl. Math., V. 6. Springer-Verlag, 1998, xvi + 531 pp, $49.95. [ISBN 0-387-98489-5] New material on nonlinear controllability via Lie-algebraic methods, variational and numerical approaches to nonlinear control, time-optimal control of linear systems, feedback linearization, nonlinear optimal feedback, controllability of neural networks, and controllability of linear systems with bounded controls. (*First Edition*, TR, February 1991.)

Applications, P. *Mathematical Morphology and its Applications to Image and Signal Processing.* Eds: Henk J.A.M. Heijmans, Jos B.T.M. Roerdink. Computat. Imaging & Vision, V. 12. Kluwer Academic, 1998, ix + 442 pp, $195. [ISBN 0-7923-5133-9] Proceedings of a 1998 symposium held in Amsterdam, The Netherlands. 5 invited and 46 contributed papers in 8 sections: Theory; Topology and Geometry; Shape Analysis and Partial Differential Equations; Connected Operators; Segmentation; Random Models and Statistical Techniques; Algorithms; Applications.

Reviewers

KB: Karla Ballman, Macalester; DB: David Bressoud, Macalester; JD: Jill Dietz, St. Olaf; BH: Bruce Hanson, St. Olaf; LCL: Loren C. Larson, St. Olaf; RL: Rob Leduc, Macalester; KS: Karen Saxe, Macalester; HS: Heidi Shierholz, St. Olaf; KES: Kay E. Smith, St. Olaf; PZ: Paul Zorn, St. Olaf.

THE MATHEMATICAL ASSOCIATION OF AMERICA



Writing in the Teaching and Learning of Mathematics

JOHN MEIER AND THOMAS RISHEL

Series: MAA Notes

Writing in the Teaching and Learning of Mathematics discusses both how to create effective writing assignments for mathematics classes and why instructors ought to consider using such assignments. The book is more than just a user's manual for what some have termed "writing to learn mathematics;" it is an argument for engaging students in a dialogue about the mathematics they are trying to learn.

The first section, "First Steps," contains chapters addressing the nuts and bolts of how to design and evaluate writing assignments. The second section, "Listening to Others," introduces ideas such as audience, narrative, prewriting and process writing, which our colleagues in writing departments have found useful. Specific examples illustrate how these are important for writing in mathematics classes. After the third section, "Major Projects," the text concludes with "Narrating Mathematics," a section making explicit what is implicit in the rest of the text: writing, speaking and thinking are all intertwined. By asking good questions and critiquing students' manuscripts in an open, yet rigorous manner, instructors can get students at any level of ability and background to a deeper awareness of the beauty and power of mathematics.

Catalog Code: NTE-48/JR
114 pp., Paperbound, 1998
ISBN 0-88385-158-X
List: $18.95 MAA Member: $14.95

Phone in Your Order Now! ☎ *1-800-331-1622*

Monday – Friday 8:30 am – 5:00 pm FAX (301) 206-9789

or mail to: The Mathematical Association of America, PO Box 91112, Washington, DC 20090-1112

Shipping and Handling: Postage and handling are charged as follows: **USA orders (shipped via UPS):** $2.95 for the first book, and $1.00 for each additional book. **Canadian orders:** $4.50 for the first book and $1.50 for each additional book. Canadian orders will be shipped within 10 days of receipt of order via the fastest available route. We do not ship via UPS into Canada unless the customer specially requests this service. Canadian customers who request UPS shipment will be billed an additional 7% of their total order. **Overseas orders:** $3.50 per item ordered for books sent surface mail. Airmail service is available at a rate of $7.00 per book. Foreign orders must be paid in US dollars through a US bank or through a New York clearinghouse. Credit Card orders are accepted for all customers.

Name ______________________________

Address ______________________________

City ______________ State _____ Zip ________

Phone ______________________________

QTY.	CATALOG CODE	PRICE	AMOUNT
______	NTE-48/JR	______	______

All orders must be prepaid with the exception of books purchased for resale by bookstores and wholesalers.

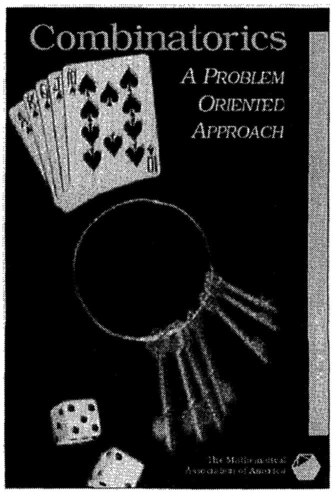
Shipping & handling ______

TOTAL ______

Payment ☐ Check ☐ VISA ☐ MasterCard

Credit Card No. ________________ Expires ___/___

Signature ______________________________



Combinatorics

A Problem Oriented Approach

Daniel Marcus

Series: Classroom Resource Materials

Textbook

Leads students quickly to the key ideas of combinatorics in a logical and proactive way . . .

This book teaches the art of enumeration, or counting, by leading the reader through a series of carfully chosen problems that are arranged strategically to introduce concepts in a logical order and in a provocative way.

The format is unique in that it combines features of a traditional textbook with those of a problem book. It is organized in eight sections, the first four of which cover the basic combinatorial entities of strings, combinations, distributions and partitions. The last four cover the special counting methods of inclusion and exclusion, recurrence relations, generating functions, and the method of Pólya and Redfield that can be characterized as "counting modulo symmetry." The subject matter is presented through a series of approximately 250 problems with connecting text where appropriate, and is supplemented by approximately 220 additional problems for homework assignments. Many applications to probability are included throughout the book.

While intended primarily for use as a text for a college-level course taken by mathematics, computer science and engineering students, the book is suitable as well for a general education course at a good liberal arts college, or for self-study.

Catalog Code: CMB/JR
156 pp., Paperbound, 1998, ISBN 0-88385-708-1
List: $28.00 MAA Member: $22.50
Solutions manual available with adoption orders.
Call 1-800-331-1622

Phone in Your Order Now! ☎ *1-800-331-1622*

Monday – Friday 8:30 am – 5:00 pm FAX (301) 206-9789

or mail to: The Mathematical Association of America, PO Box 91112, Washington, DC 20090-1112

Shipping and Handling: Postage and handling are charged as follows: **USA orders (shipped via UPS):** $2.95 for the first book, and $1.00 for each additional book. **Canadian orders:** $4.50 for the first book and $1.50 for each additional book. Canadian orders will be shipped within 10 days of receipt of order via the fastest available route. We do not ship via UPS into Canada unless the customer specially requests this service. Canadian customers who request UPS shipment will be billed an additional 7% of their total order. **Overseas orders:** $3.50 per item ordered for books sent surface mail. Airmail service is available at a rate of $7.00 per book. Foreign orders must be paid in US dollars through a US bank or through a New York clearinghouse. Credit Card orders are accepted for all customers.

Name ______________________

Address ______________________

City ____________ State ______ Zip ______

Phone ______________________

Qty.	Catalog Code	Price	Amount
______	CMB/JR	______	______

All orders must be prepaid with the exception of books purchased for resale by bookstores and wholesalers.

Shipping & handling ______

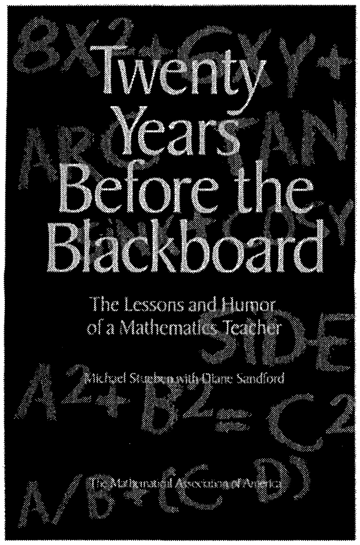
TOTAL ______

Payment ☐ Check ☐ VISA ☐ MasterCard

Credit Card No. ______________ Expires ___/___

Signature ______________________

THE MATHEMATICAL ASSOCIATION OF AMERICA



Twenty Years Before the Blackboard

The Lessons and Humor of a Mathematics Teacher

Michael Stueben with Diane Sandford

Series: Spectrum

A perfect gift for the new teacher. . . or for anyone interested in the teaching of mathematics.

This book is the legacy of twenty years of mathematics teaching. During this time, the author searched for motivation techniques, mnemonics, insightful proofs, and serious applications of humor to aid his teaching. The result is this book: part philosophy, part humor, and part biography. Readers will be amused and enlightened on every page.

Mr. Stueben shows how he has used humor and wordplay to motivate his students. The book is filled with wonderful problems and proofs, as well as the author's insights about how to approach teaching problem solving to high school students. Sections of the book also treat the use of calculators and computers in the classroom. A section on mnemonics shows how teachers can use memory aids to help their students learn and retain material.

All in all, *Twenty Years Before the Blackboard* provides a goldmine of ideas for the classroom teacher. Although Mr. Stueben taught at the high school level, his book is an excellent "methods" book for mathematics teachers at all levels.

Read what Martin Gardner has to say about this fascinating book:

It's been decades since I read so entertaining a book about mathematics. The book is a treasure-trove of mathematical jokes, rhymes, anecdotes, word play, mnemonics, and beautiful proofs. For teachers there is an abundance of wise advice based on the author's twenty years in high school teaching. Mathematicians at all levels, from amateurs to college professors will not only chuckle over its gems, but learn much they did not know before. —Martin Gardner

Catalog Code: TYB/JR98
174 pp., Paperbound, 1998, ISBN 0-88385-525-9
List: $29.50 MAA Member: $23.50

Phone in Your Order Now! ☎ *1-800-331-1622*

Monday – Friday 8:30 am – 5:00 pm FAX (301) 206-9789

or mail to: The Mathematical Association of America, PO Box 91112, Washington, DC 20090-1112

Shipping and Handling: Postage and handling are charged as follows: **USA orders (shipped via UPS):** $2.95 for the first book, and $1.00 for each additional book. **Canadian orders:** $4.50 for the first book and $1.50 for each additional book. Canadian orders will be shipped within 10 days of receipt of order via the fastest available route. We do not ship via UPS into Canada unless the customer specially requests this service. Canadian customers who request UPS shipment will be billed an additional 7% of their total order. **Overseas orders:** $3.50 per item ordered for books sent surface mail. Airmail service is available at a rate of $7.00 per book. Foreign orders must be paid in US dollars through a US bank or through a New York clearinghouse. Credit Card orders are accepted for all customers.

Name ____________________

Address ____________________

City ____________ State _____ Zip _______

Phone ____________________

QTY.	CATALOG CODE	PRICE	AMOUNT
______	TYB/JR98	______	______

All orders must be prepaid with the exception of books purchased for resale by bookstores and wholesalers.

Shipping & handling ______

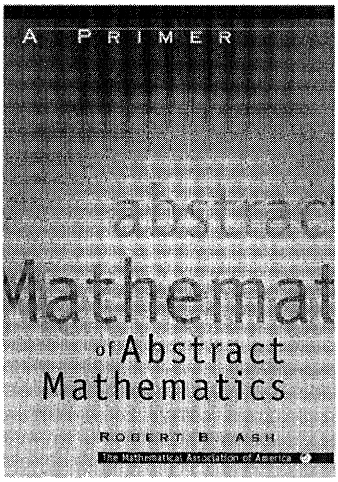
TOTAL ______

Payment ☐ Check ☐ VISA ☐ MasterCard

Credit Card No. ____________________ Expires ___/___

Signature ____________________

THE MATHEMATICAL ASSOCIATION OF AMERICA



A Primer of Abstract Mathematics

Robert Ash

Series: Classroom Resource Materials

A Primer of Abstract Mathematics prepares the reader to cope with abstract mathematics, specifically abstract algebra. It can serve as a text for prospective mathematics majors, as well as for those students taking or preparing to take a first course in abstract algebra, or those in applied fields who need experience in dealing with abstract mathematical ideas.

Learning any area of abstract mathematics involves writing formal proofs, but it is equally important to think intuitively about the subject and to express ideas clearly and cogently. The author aids intuition by keeping proofs short and as informal as possible, using concrete examples which illustrate all the features of the general case, and by giving heuristic arguments when a formal development would take too long. The text can serve as a model on how to write mathematics for an audience with limited experience in formalism and abstraction.

Ash introduces several expository innovations in *A Primer of Abstract Mathematics.* He presents an entirely informal development of set theory that gives students the basic results that they will need in algebra. The chapter which presents the theory of linear operators introduces the Jordan Canonical Form right at the beginning, with a proof of existence at the end of the chapter.

Contents:

Catalog Code: BMA/JR
188 pp., Paperbound, 1998
ISBN 0-88385-709-X
List: $27.95 MAA Member: $21.95

Phone in Your Order Now! ☎ *1-800-331-1622*

Monday – Friday 8:30 am – 5:00 pm FAX (301) 206-9789

or mail to: The Mathematical Association of America, PO Box 91112, Washington, DC 20090-1112

Shipping and Handling: Postage and handling are charged as follows: **USA orders (shipped via UPS):** $2.95 for the first book, and $1.00 for each additional book. **Canadian orders:** $4.50 for the first book and $1.50 for each additional book. Canadian orders will be shipped within 10 days of receipt of order via the fastest available route. We do not ship via UPS into Canada unless the customer specially requests this service. Canadian customers who request UPS shipment will be billed an additional 7% of their total order. **Overseas orders:** $3.50 per item ordered for books sent surface mail. Airmail service is available at a rate of $7.00 per book. Foreign orders must be paid in US dollars through a US bank or through a New York clearinghouse. Credit Card orders are accepted for all customers.

Name ______________________

Address ______________________

City ____________ State _____ Zip ________

Phone ______________________

QTY.	CATALOG CODE	PRICE	AMOUNT
_____	BMA/JR	_____	_____
		Shipping & handling	_____
		TOTAL	_____

All orders must be prepaid with the exception of books purchased for resale by bookstores and wholesalers.

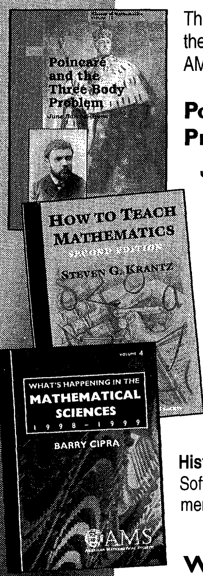
Payment ☐ Check ☐ VISA ☐ MasterCard

Credit Card No. ______________ Expires ___/___

Signature ______________________

AMERICAN MATHEMATICAL SOCIETY

Bestselling General Interest Titles from the AMS



These bestselling selections provide vital and informative historical, biographical, and educational perspectives in the field of mathematics and are frequently adopted as course texts. Choose from the titles below or browse the AMS Bookstore at www.ams.org/bookstore/ to find more General Interest works that best meet your needs.

Poincaré and the Three Body Problem

June Barrow-Green, *The Open University, Milton Keynes, UK*

Delightful and interesting to read ... will help professors ... provide some very interesting (and needed) historical background to their lectures. Any serious student of mathematical history will enjoy this treatise.

—Applied Mechanics Reviews

Co-published with the London Mathematical Society. Members of the LMS may order directly from the AMS at the AMS member price. The LMS is registered with the Charity Commissioners.

History of Mathematics, Volume 11; 1997; 272 pages; Softcover; ISBN 0-8218-0367-0; List $39; All AMS members $31; Order code HMATH/11MM94

What's Happening in the Mathematical Sciences, 1998–1999

Barry Cipra

Praise for *What's Happening in the Mathematical Sciences*

Another choice of new exciting developments in mathematics. These volumes really deserve a large audience, students as well as researchers will be fascinated by the insights and overviews presented.

—Zentralblatt für Mathematik

Cover picture, detail from "Wave–Particle Duality", was created and provided by artist Mel Fisher. Reproduced with permission.

What's Happening in the Mathematical Sciences, Volume 4; 1999; 126 pages; Softcover; ISBN 0-8218-0766-8; List $14; Order code HAPPENING/4MM94

The Man Who Loved Only Numbers

The Story of Paul Erdős and the Search for Mathematical Truth

Paul Hoffman

A publication of Hyperion Press.

This book opens doors on a world and characters that are often invisible. It is interesting that Hoffman, Erdős and others in the book remember the mathematical tidbit that first intrigued them and bound them to this world. Possibly a future scientist or mathematician, or future scientific writer, will remember something in this book that way.

—New York Times Book Review

Distributed worldwide by the American Mathematical Society.

1998; 302 pages; Hardcover; ISBN 0-7868-6362-5; List $23; All AMS members $16; Order code MLONMM94

How to Teach Mathematics

Second Edition

Steven G. Krantz, *Washington University, St. Louis, MO*

Praise for the First Edition ...

An original contribution to the educational literature on teaching mathematics at the post-secondary level. The book itself is an explicit proof of the author's claim "teaching can be rewarding, useful, and fun".

—Zentralblatt für Mathematik

This expanded edition of the original bestseller, *How to Teach Mathematics*, offers hands-on guidance for teaching mathematics in the modern classroom setting. Twelve appendices have been added that are written by experts who have a wide range of opinions and viewpoints on the major teaching issues.

1999; 307 pages; Softcover; ISBN 0-8218-1398-6; List $24; All AMS members $19; Order code HTM/2MM94

Techniques of Problem Solving

Steven G. Krantz

It may be an enjoyable task for high school undergraduate mathematics students, their teachers and people interested in the field, to read the book and to learn from it by working on the challenging ideas which are provided throughout the text.

—Zentralblatt für Mathematik

The purpose of this book is to teach the basic principles of problem solving, including both mathematical and non-mathematical problems. A *Solutions Manual* to most end-of-chapter exercises is available.

1997; 465 pages; Softcover; ISBN 0-8218-0619-X; List $29; All AMS members $23; Order code TPSMM94

A Gentle Introduction to Game Theory

Saul Stahl, *University of Kansas, Lawrence*

This volume is based on courses given by the author at the University of Kansas. The exposition is "gentle" because it requires only some knowledge of coordinate geometry; linear programming is not used. It is "mathematical" because it is more concerned with the mathematical solution of games than with their applications.

Mathematical World, Volume 13; 1999; 176 pages; Softcover; ISBN 0-8218-1339-0; List $25; All AMS members $20; Order code MAWRLD/13MM94

AMS
AMERICAN MATHEMATICAL SOCIETY

All prices subject to change. Charges for delivery are $3.00 per order. For optional air delivery outside of the continental U. S., please include $6.50 per item. *Prepayment required.* Order from: **American Mathematical Society**, P. O. Box 5904, Boston, MA 02206-5904, USA. For credit card orders, fax 1-401-455-4046 or call toll free 1-800-321-4AMS (4267) in the U. S. and Canada, 1-401-455-4000 worldwide. Or place your order through the AMS bookstore at www.ams.org/bookstore/. Residents of Canada, please include 7% GST.